OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

August 19, 2019

Shawn Musgrave
MuckRock News
Dept MR 15851
PO Box 55819
Boston, MA 02205-5819

Subject: OIG Freedom of Information Act Request No. 2015-087
Final Response

Dear Mr. Musgrave:

This responds to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS) Office of Inspector General (OIG), dated January 29, 2015, seeking "all communications and correspondence (including emails with all attachments) sent to or from the DHS OIG office regarding the classification of information within OIG-15-18, 'Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport,' as Sensitive Security Information." Your request was received in this office on January 29, 2015.

DHS-OIG conducts independent investigations, audits, inspections, and special reviews of DHS personnel, programs, and operations to detect and deter waste, fraud, and abuse, and to promote integrity, economy, and efficiency within DHS. In response to your request, a search of the DHS-OIG Office of Information Technology (ITD) was conducted. That search resulted in the enclosed records responsive to your request. We reviewed the responsive records under the FOIA to determine whether they may be disclosed to you. Based on that review, this office is providing the following:

248 page(s) are released in full (RIF);
62 page(s) are released in part (RIP);
3 page(s) are withheld in full (WIF);
72 page(s) are duplicate copies of material already processed;
60 page(s) were referred to another entity.

The exemptions cited for withholding records or portions of records are marked below.

Freedom of Information Act, 5 U.S.C. § 552			**Privacy Act, 5 U.S.C. § 552a**
□ 552(b)(1)	☒ 552(b)(5)	☒ 552(b)(7)(C)	□ 552a(j)(2)
□ 552(b)(2)	☒ 552(b)(6)	□ 552(b)(7)(D)	□ 552a(k)(2)
□ 552(b)(3)	□ 552(b)(7)(A)	□ 552(b)(7)(E)	□ 552a(k)(5)
□ 552(b)(4)	□ 552(b)(7)(B)	□552(b)(7)(F)	□ Other:

OIG redacted from the enclosed documents, names and identifying information of third parties to protect the identities of these individuals. Absent a Privacy Act waiver, the release of such information concerning the third parties named in these records would result in an unwarranted invasion of personal privacy in violation of the Privacy Act. Information is also protected from disclosure pursuant to Exemptions (b)(5), (b)(6) and (b)(7)(C) of the FOIA further discussed below.

Exemption 5, 5 U.S.C. § 552(b)(5)

Exemption 5 of the FOIA protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." 5 U.S.C. § 552(b)(5). DHS-OIG is invoking the attorney work product privilege of Exemption 5 to protect information that falls within that privilege's domain.

Exemption 6, 5 U.S.C. § 552(b)(6)

Exemption 6 allows withholding of "personnel and medical files and *similar files* the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6)(emphasis added). DHS-OIG is invoking Exemption 6 to protect the names of government employees and any information that could reasonably be expected to identify such individuals.

Exemption 7(C), 5 U.S.C. § 552(b)(7)(C)

Exemption 7(C) protects from public disclosure "records or information compiled for law enforcement purposes . . . [if disclosure] could reasonably be expected to cause an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C). DHS-OIG is invoking Exemption 7(C) to protect the identities of government employees, and any information contained in these investigative records that could reasonably be expected to identify those individuals.

Referral

Additionally, 60 pages have been referred to Transportation Security Administration (TSA), a DHS component. TSA will process the record under the FOIA and respond to you directly. Should you wish to contact TSA you may write to:

U.S. Department of Homeland Security (DHS)
Transportation Security Administration (TSA)
FOIA Officer
Freedom of Information Act (FOIA) Branch
701 S. 12th Street
Arlington, VA 20598-6020

or you may call 571-227-2300.

Appeal

You have the right to appeal this response.[1] Your appeal must be in writing and received within 90 days of the date of this response. Please address any appeal to:

FOIA/PA Appeals Unit
DHS-OIG Office of Counsel
Stop 0305
245 Murray Lane, SW
Washington, DC 20528-0305

Both the envelope and letter of appeal must be clearly marked, "Freedom of Information Act/Privacy Act Appeal." Your appeal letter must also clearly identify the DHS-OIG's response. Additional information on submitting an appeal is set forth in the DHS regulations at 6 C.F.R. § 5.8.

Assistance and Dispute Resolution Services

Should you need assistance with your request, you may contact DHS-OIG's FOIA Public Liaison. You may also seek dispute resolution services from our FOIA Public Liaison. You may contact DHS-OIG's FOIA Public Liaison in any of the following ways:

[1] For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. 5 U.S.C. 552(c) (2006 & Supp. IV 2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

FOIA Public Liaison
DHS-OIG Counsel
STOP 0305
245 Murray Lane, SW
Washington, DC 20528-0305
Phone: 202-254-4001
Fax: 202-254-4398
E-mail: foia.oig@oig.dhs.gov

Additionally, the 2007 FOIA amendments created the Office of Government Information Services (OGIS) to offer mediation services to resolve disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Using OGIS services does not affect your right to pursue litigation. You may contact OGIS in any of the following ways:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road - OGIS
College Park, MD 20740-6001
E-mail: ogis@nara.gov
Web: https://ogis.archives.gov
Telephone: 202-741-5770
Fax: 202-741-5769
Toll-free: 1-877-684-6448

If you have any questions about this response, please contact Steven Phelps, FOIA/PA Disclosure Specialist, at 202-981-6338.

Sincerely,

Steven G. Phelps

Steven G. Phelps
FOIA/PA Disclosure Specialist

Enclosure(s)

Copy of FOIA Request

From: 15851-29740219@requests.muckrock.com
To: FOIA OIG
Subject: Freedom of Information Request: DHS OIG - TSA communications re: JFK audit classification
Date: Thursday, January 29, 2015 7:49:04 PM

January 29, 2015
Department of Homeland Security Office of Inspector General
245 Murray Lane SW
Mail Stop - 0305
Washington, D.C. 20528-0305

To Whom It May Concern:

This is a request under the Freedom of Information Act. I hereby request the following records:

All communications and correspondence (including emails with all attachments) sent to or from the DHS OIG office regarding the classification of information within OIG-15-18, "Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport," as Sensitive Security Information (SSI).

Please include all communications/correspondence from July 1, 2014 through the date this request is processed.

This includes, at minimum, the communications outlined in the following passage from the redacted version of the above report as published at the DHS OIG website (see http://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-18_Jan14.pdf), in which Inspector General John Roth describes the procedural history of the report:

"The procedural history of this report elicits an unfortunate commentary on the manner in which the Department handled this matter and bears review:

-We provided a draft of this report on July 22, 2014 to the Chief Information Officer for review. Pursuant to Department of
Homeland Security Directive 077-01, Follow-up, and Resolution for Office of Inspector General Report Recommendations, we asked for agency comments, including a sensitivity review, within 30 days of receipt of the draft. This would have made the report due on or about August 22, 2014. Almost a week later, on August 27, 2014, the DHS Chief of Staff requested an extension to provide a
response and technical comments. I granted the extension until September 17, 2014.

-On October 20, 2014, nearly 60 days after the original due date for agency comments, the Departmental GAO-OIG Liaison Office finally conveyed to us TSA's response to our request for a sensitivity review by marking several passages in the report as SSI. I disagree with this determination.

- On November 19, 2014, I sent a formal challenge memo to TSA Administrator John Pistole expressing my disagreement. Administrator Pistole had authority over all TSA programs and operations, including oversight of the SSI programs, and is my counterpart in DHS' leadership.

- Having received no reply, on December 16, 2014, I wrote to Administrator Pistole a second time, noting that this report had
languished as a result of TSA's sensitivity review, and again requesting that he remove the SSI deletions from the report. As
with the November 19, 2014 letter, I received no reply.

-Finally, on January 13, 2015, over five months after submitting the report for sensitivity review, and two months after writing to Administrator Pistole, I received a decision, not from the Acting TSA Administrator, but from the head of the SSI program office - the very same office that initially and improperly marked the information as SSI. Not surprisingly, the office affirmed its original
redaction to the report."

To be clear, this request is not limited to the above, but also includes any communications/correspondence sent following the publication of the DHS OIG redacted report.

I also request that fees be waived as I believe this request is in the public interest. The requested documents will be made available to the general public free of charge as part of the public information service at MuckRock.com, processed by a representative of the news media/press and is made in the process of news gathering and not for commercial usage.

I furthermore request a fee waiver on the basis of my status as a journalist who has covered inspectors general extensively. Here is a selection of my published articles reviewing IG reports:

http://motherboard.vice.com/read/the-air-force-says-it-needs-precisely-52-new-reaper-drones-cant-explain-why

http://motherboard.vice.com/read/the-us-spent-360-million-on-border-drones-thanks-to-this-flimsy-report

http://motherboard.vice.com/blog/the-feds-have-no-idea-whos-flying-drones

https://www.muckrock.com/news/archives/2013/jul/01/cia-nypd-relationship-report-and-daisy-chain-foias/

https://www.muckrock.com/news/archives/2014/feb/18/dhs-vancouver-olympics-social-media/

In addition to the above, I have also been published in a handful of other national media outlets:

https://www.themarshallproject.org/2014/12/03/the-pentagon-finally-details-its-weapons-for-cops-giveaway

https://www.bostonglobe.com/metro/2013/04/08/big-brother-better-police-work-new-technology-automatically-runs-license-plates-everyone/1qoAoFfgp31UnXZT2CsFSK/story.html

https://news.vice.com/article/fbi-agent-who-killed-boston-bombing-suspects-friend-was-twice-accused-of-police-brutality

In the event that fees cannot be waived, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 20 business days, as the statute requires.

Sincerely,

Shawn Musgrave

Filed via MuckRock.com
E-mail (Preferred): 15851-29740219@requests.muckrock.com

For mailed responses, please address (see note):
MuckRock News
DEPT MR 15851
PO Box 55819
Boston, MA 02205-5819

PLEASE NOTE the new address as well as the fact that improperly addressed (i.e., with the requester's name rather than MuckRock News) requests might be returned by the USPS as undeliverable.

DOCUMENTS

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

60 PAGE(S)

are referred to TSA for processing
and direct response to requester.
[pages 1,7,14-15,18,20,22,29,32-33,35,37,40,42,44-47,49-54,220,221,224-225,227-228,231-232,234-236,238,256,280-282,483,485-486,551,555,565-566,588-589,598-599,613-614,628,633-634,647-648,660,664]

From: Balaban, Dorothy
Sent: Friday, January 09, 2015 01:24 PM
To: Huiswoud, Sharon
Subject: FW: Memo to TSA re JFK Intl Airport

FYI

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254 (b)(6)

Notary Public for the District of Columbia

From: Balaban, Dorothy
Sent: Friday, November 21, 2014 5:59 PM
To: Harsche, Richard; Tsang, Chiu-Tong
Subject: Memo to TSA re JFK Intl Airport

All,

This memo has been sent to the Administrator. Please feel free to share with your counterparts at TSA.

I made the two requested edits to the memo.

Have a great weekend.

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254 (b)(6)

Notary Public for the District of Columbia

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

NOV 1 9 2014

MEMORANDUM FOR: The Honorable John Pistole
Administrator
Transportation Security Administration

FROM: John Roth John Roth
Inspector General

SUBJECT: Office of Inspector General's Challenge to Sensitive Security Information Office's Request to Mark OIG report: *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport* as SSI
OIG *Project No: 14-082-ITA-DHS*

The Inspector General Act requires the Office of Inspector General (OIG) to conduct audits and investigations that promote the economy, efficiency, and effectiveness of DHS programs and operations, and to inform the Secretary, Congress, and the public about any problems and deficiencies we identify. Our ability to issue reports to the public that are transparent, without unduly restricting information, is key to accomplishing our mission.

I am concerned that the Department's review and response to our draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport*, indicated that several statements within the report were determined to be Sensitive Security Information (SSI). I disagree with this determination and I am submitting this formal challenge according to procedures outlined in DHS Management Directive MD 11056.1, Sensitive Security Information. Under DHS MD 11056.1.F.2, a formal challenge may be submitted, in writing, to the person who made the SSI markings or to the SSI Office.

We issued the draft report, *Technical Security Evaluation of DHS Activities at JFK International Airport,* to the Department on July 22, 2014. On August 6, 2014, a SSI Senior Program Analyst, provided a response and marked as SSI several passages in this report. See Attachment A for a copy of this draft report with the suggested SSI content highlighted. I recognize the SSI Office's process to identify and safeguard SSI information. However, I believe the information in our draft report was

improperly marked as SSI and I am challenging this determination based on the following:

First, the same or similar information as that marked SSI in the current draft report was disclosed to the public in previously released DHS OIG and GAO reports. The Department reviewed and approved the content of these previously released reports and did not determine at that time that the information was SSI. For example:

- On page 5 of our draft report, we discuss physical security issues in TSA's space at JFK airport. The SSI Office marked this information as SSI based on 49 C.F.R. § 1520.5(b) (5). I challenge this request. In GAO audit report *General Aviation: Security Assessments at Selected Airports*, GAO-11-298 dated May 2011, GAO published similar information. Specifically, the GAO report discusses and reports the security measures and potential vulnerabilities at selected airports. (page 7, Attachment B)
- Also, on page 5 of our draft report, we display a picture of TSA equipment in a corridor accessible by unsecured double doors to public area prior to TSA terminal security checkpoint. The SSI Office marked this picture SSI. I challenge this request. This is a picture of IT equipment similar to the IT equipment pictured in figures 4, 5, and 6 of our draft report, yet the SSI Office did not mark those figures SSI. This item shows an example of a TSA equipment cabinet that is in an area accessible to non TSA staff and the public. This risk can be controlled and eliminated by TSA simply securing the terminal corridor from unauthorized access. In addition, our report did not provide the specific location of this cabinet.
- On pages 14 and 21 of our draft report, the SSI office marked one sentence on each page as SSI information. These sentences are located in the TSA (page 14) and CBP (page 21) Patch Management Sections of our report. I challenge this request. Similar or the same wording was used in our last two publically released technical security airport reviews at Dallas Ft. Worth (*Audit of Security Controls for DHS Information Technology Systems at Dallas/Ft. Worth International Airport*, OIG-14-132) and Atlanta's Hartsfield (*Technical Security Evaluation of DHS Activities at Hartsfield Jackson Atlanta International Airport*, OIG-13-104) airports. (pages 10, 18, and 25 in Attachment C and pages 10, 20, and 31 in Attachment D)

- Also on pages 14 and 21 of our draft report, the SSI office marked information in the tables in the TSA and CBP Patch Management sections of the report as SSI information. I challenge this request. Similar content in the same table format was reported in our last two publically released DHS OIG audit reports on Dallas/Ft. Worth, OIG-14-132, and Atlanta Hartsfield airports OIG-13-104. (pages 10, 18, and 25 in Attachment C and pages 10, 20, and 31 in Attachment D)

Second, although the SSI Office marked information in the TSA and CBP Patch Management sections of the draft report as SSI, the SSI Office did not mark the same information in the ICE section of the same report as SSI. Specifically, the ICE section of the draft report includes the same table and wording regarding scanning vulnerabilities that is in the TSA and CBP sections. However, the SSI office did not mark the ICE information as SSI. The SSI determination appears to be inconsistently applied.

Further, even if past reports had not released similar information, I still do not believe its release in this report would be detrimental to transportation security. For example, the language marked SSI reveals generic vulnerabilities that are common to virtually all systems. In addition, the descriptions of the vulnerabilities are not specific enough to be detrimental.

For these reasons, I am requesting that you reconsider and remove your SSI markings from our draft report. These markings impede the effectiveness and transparency of our office. I feel that based on the reasons I have outlined above, our OIG report, *Technical Security Evaluation of DHS Activities at JFK International Airport,* should be released in its entirety in the public Domain.

I appreciate your attention to this matter. Please feel free to contact me with any questions.

cc: Jim Crumpacker, Director, DHS GAO/OIG Liaison Office
Shelly Peterson, Audit Liaison for the Chief Information Officer
Susan Perkins, TSA, Audit Liaison
Tamara Lilly, DHS CISO, Audit Liaison
John Buckley, CBP, CISO
Judy Wright, CBP, Audit Liaison
Tom DeBiase, ICE, Acting CISO

Joanna Perkins, ICE, Audit Liaison
Jill Vaughan, TSA, CISO
Thomas Feltrin, TSA, Audit Liaison
Doug Blair, SSI Program Chief
Rob Metzler, Senior Analyst

Cc: Grady, Sharell; Dale, Beverly A.
Subject: Fw: Memo to TSA re JFK Intl Airport

Hi Susan-

Attached is the original email that was sent to Mr. Pistole. It was from the IG, Mr. Roth and mailed by his assistant Dorothy Balaban.

Sharon L. Huiswoud
Director, Information Systems Division
DHS OIG
202-25 (b)(6)

From: Balaban, Dorothy
Sent: Friday, January 09, 2015 01:24 PM
To: Huiswoud, Sharon
Subject: FW: Memo to TSA re JFK Intl Airport

FYI

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254 (b)(6)

Notary Public for the District of Columbia

From: Balaban, Dorothy
Sent: Friday, November 21, 2014 5:59 PM
To: Harsche, Richard; Tsang, Chiu-Tong
Subject: Memo to TSA re JFK Intl Airport

All,

This memo has been sent to the Administrator. Please feel free to share with your counterparts at TSA.

I made the two requested edits to the memo.

Have a great weekend.

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-25 (b)(6)

Notary Public for the District of Columbia

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

4 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

I made the two requested edits to the memo.

Have a great weekend.

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-25 (b)(6)

Notary Public for the District of Columbia

Unknown

From: Harsche, Richard
Sent: Friday, January 09, 2015 2:53 PM
To: Huiswoud, Sharon
Subject: RE: OIG-15-18, "Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport-Sensitive Security Information." --REQUEST FOR MEMORANDUM

Can you call me? 202-254 (b)(6)

From: Huiswoud, Sharon
Sent: Friday, January 09, 2015 2:52 PM
To: Harsche, Richard
Subject: Re: OIG-15-18, "Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport-Sensitive Security Information." --REQUEST FOR MEMORANDUM

Dottie forwarded the email

Sharon L. Huiswoud
Director, Information Systems Division
DHS OIG
202-254 (b)(6)

From: Harsche, Richard
Sent: Friday, January 09, 2015 02:43 PM
To: Huiswoud, Sharon
Subject: RE: OIG-15-18, "Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport-Sensitive Security Information." --REQUEST FOR MEMORANDUM

There should be a record in PTS.

From: Huiswoud, Sharon
Sent: Friday, January 09, 2015 1:37 PM
To: Harsche, Richard
Subject: Fw: OIG-15-18, "Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport-Sensitive Security Information." --REQUEST FOR MEMORANDUM
Importance: High

Fyi..TSA audit liaison is saying they never received original challenge memo. I asked Dottie if she has the original email that was sent to Pistole

Sharon L. Huiswoud
Director, Information Systems Division
DHS OIG
202-254 (b)(6)

Office of Public Affairs
Office of Inspector General
Department of Homeland Security
Phone: 202.254.4100
www.oig.dhs.gov | Twitter: @DHSOIG

(b)(6)
(b)(6)
(b)(6) Crumpacker, Jim; (b)(6) ESEC DHS Reports; (b)(6)
GAO-OIG Liaison; (b)(6) @HQ.DHS.GOV
Cc: Huiswoud, Sharon; Grady, Sharell; Dale, Beverly A.; Shappee, Frederick; Balaban, Dorothy; Hurley, Kim; OIG's DHS Liaison; DHS-OIG Office of Public Affairs; DHS-OIG Office of Legislative Affairs; Manduzio, James; Nadon, Patrick
Subject: OIG-15-18, "Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport-Sensitive Security Information."

Good Morning,

Attached is the final report, OIG-15-18, ***"Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport-Sensitive Security Information."*** The SSI version of this document is password protected and an email containing the password will be forwarded to you shortly.

***This is an advance copy that has not been made public by the DHS OIG. Do Not Distribute Without OIG Authorization.** The projected date for delivery to **Congress is January 15, 2015**. The projected date for **Web posting is January 19, 2015**. Actual dates may differ please contact OIG to confirm.

Thank you,

Office of Public Affairs
Office of Inspector General
Department of Homeland Security
Phone: 202.254.4100
www.oig.dhs.gov **l** Twitter: @DHSOIG

Attached is the original email that was sent to Mr. Pistole. It was from the IG, Mr. Roth and mailed by his assistant Dorothy Balaban.

Sharon L. Huiswoud
Director, Information Systems Division
DHS OIG
202-254 (b)(6)

From: Balaban, Dorothy
Sent: Friday, January 09, 2015 01:24 PM
To: Huiswoud, Sharon
Subject: FW: Memo to TSA re JFK Intl Airport

FYI

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254- (b)(6)

Notary Public for the District of Columbia

From: Balaban, Dorothy
Sent: Friday, November 21, 2014 5:59 PM
To: Harsche, Richard; Tsang, Chiu-Tong
Subject: Memo to TSA re JFK Intl Airport

All,

This memo has been sent to the Administrator. Please feel free to share with your counterparts at TSA.

I made the two requested edits to the memo.

Have a great weekend.

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-25 (b)(6)

Notary Public for the District of Columbia

Requester’s Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

4 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

Attached is the revised final report, OIG-15-18, ***"Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport."*** The SSI version of this document is password protected. An email containing the password will be forwarded to you shortly.

Thank you,

Office of Public Affairs
Office of Inspector General
Department of Homeland Security
Phone: 202.254.4100
www.oig.dhs.gov **l** Twitter: @DHSOIG

Audit Liaison Division

Integrity | Partnership | Support

Audit
Liaison
Division

Integrity | Partnership | Support

Audit
Liaison
Division

Integrity | Partnership | Support

Audit
Liaison
Division

Integrity | Partnership | Support

Audit
Liaison
Division

Integrity | Partnership | Support

Audit
Liaison
Division

Integrity | Partnership | Support

Please let us know.

-----Original Appointment-----
From: Burke, Kevin
Sent: Thursday, March 31, 2016 11:21 AM
To: Perkins, Susan
Subject: Accepted: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program
When: Tuesday, April 05, 2016 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Bridge Line: (b)(6)

Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

(b)(6)

If TSA would prefer to not discuss SSI issues over the phone, Charles and I can go to HQ.

Please let us know.

-----Original Appointment-----
From: Burke, Kevin
Sent: Thursday, March 31, 2016 11:21 AM
To: (b)(6)
Subject: Accepted: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program
When: Tuesday, April 05, 2016 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Bridge Line (b)(6)

Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

(b)(6)

If TSA would prefer to not discuss SSI issues over the phone, Charles and I can go to HQ.

Please let us know.

-----Original Appointment-----
From: Burke, Kevin
Sent: Thursday, March 31, 2016 11:21 AM
To: (b)(6)
Subject: Accepted: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program
When: Tuesday, April 05, 2016 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Bridge Line (b)(6)

Unknown

From: Burke, Kevin
Sent: Tuesday, April 05, 2016 1:38 PM
To: Huiswoud, Sharon
Cc: Twitty, Charles
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Yes…will do

From: Huiswoud, Sharon
Sent: Tuesday, April 05, 2016 1:36 PM
To: Burke, Kevin
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Ok…I guess we need to let Sondra know what happened on the call. Can you write a brief summary of the discussion so she can know before Roth says something to her.

Sharon L. Huiswoud
Director
Information Systems and Acquisitions Division
Office of IT Audits
Department of Homeland Security
Office of Inspector General
office: 202-254 (b)(6);(b)(7)(
cell: 202-497- (b)(6);(b)(7)(C)

From: Burke, Kevin
Sent: Tuesday, April 05, 2016 1:35 PM
To: Bryant, Tania
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Thanks.

We were going to ask TSA for the updated redaction of the three sentences that was mentioned in the teleconference. Should we hold off on asking?

From: Bryant, Tania
Sent: Tuesday, April 05, 2016 1:34 PM
To: Burke, Kevin
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

From: Burke, Kevin
Sent: Thursday, March 31, 2016 1:10 PM
To: (b)(6)
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

(b)(6)

If TSA would prefer to not discuss SSI issues over the phone, Charles and I can go to HQ.

Please let us know.

-----Original Appointment-----
From: Burke, Kevin
Sent: Thursday, March 31, 2016 11:21 AM
To: Perkins, Susan
Subject: Accepted: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program
When: Tuesday, April 05, 2016 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Bridge Line (b)(6)

(b)(6)

Desk: 571-227 (b)(6)
Mobile: 202-7

From: Burke, Kevin
Sent: Thursday, March 31, 2016 1:10 PM
To: (b)(6)
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

(b)(6)

If TSA would prefer to not discuss SSI issues over the phone, Charles and I can go to HQ.

Please let us know.

-----Original Appointment-----
From: Burke, Kevin
Sent: Thursday, March 31, 2016 11:21 AM
To: (b)(6)
Subject: Accepted: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program
When: Tuesday, April 05, 2016 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Bridge Line (b)(6)

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

3 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

Requester's Name: Shawn Musgrave

FOIA/PA NO.: 2015-087

4 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

Unknown

From:	Burke, Kevin
Sent:	Thursday, April 07, 2016 7:23 AM
To:	Bryant, Tania
Cc:	Huiswoud, Sharon; Twitty, Charles
Subject:	RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program
Attachments:	040416 SSI - IT Management Challenges Continue in TSA's Security Technol....pdf

Sorry all…here is the new redaction request.

From: Bryant, Tania
Sent: Wednesday, April 06, 2016 7:30 AM
To: Burke, Kevin
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Kevin,

There was no attachment. ☺ I do that all the time!

Tania

From: Burke, Kevin
Sent: Tuesday, April 05, 2016 3:51 PM
To: Bryant, Tania
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Tania,

Attached is the updated redaction request from TSA. The only change is to the last sentence in the 2nd paragraph on page 7. Less is redacted in that sentence.

From: Bryant, Tania
Sent: Tuesday, April 05, 2016 1:37 PM
To: Burke, Kevin
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

No, I'll just forward the update to Laurel when you get it back.

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

3 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

Unknown

From:	Twitty, Charles
Sent:	Thursday, April 07, 2016 8:17 AM
To:	Burke, Kevin
Cc:	Twitty, Charles
Subject:	RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Thanks

From: Burke, Kevin
Sent: Thursday, April 07, 2016 8:15 AM
To: Twitty, Charles
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Yes…AS5.d

From: Twitty, Charles
Sent: Thursday, April 07, 2016 8:14 AM
To: Burke, Kevin
Cc: Twitty, Charles
Subject: FW: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Kevin,

Did you put the write-up of the redacted meeting in TeamMate?

Thanks,
Charles

From: Burke, Kevin
Sent: Tuesday, April 05, 2016 3:51 PM
To: Bryant, Tania
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Tania,

Attached is the updated redaction request from TSA. The only change is to the last sentence in the 2nd paragraph on page 7. Less is redacted in that sentence.

From: Bryant, Tania

Sent: Tuesday, April 05, 2016 1:37 PM
To: Burke, Kevin
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

No, I'll just forward the update to Laurel when you get it back.

From: Burke, Kevin
Sent: Tuesday, April 05, 2016 1:35 PM
To: Bryant, Tania
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Thanks.

We were going to ask TSA for the updated redaction of the three sentences that was mentioned in the teleconference. Should we hold off on asking?

From: Bryant, Tania
Sent: Tuesday, April 05, 2016 1:34 PM
To: Burke, Kevin
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

Thank you, Kevin.

Laurel will be discussing the redaction matter with the IG. I will keep you updated.

Tania

From: Burke, Kevin
Sent: Tuesday, April 05, 2016 12:28 PM
To: Bryant, Tania
Cc: Twitty, Charles; Huiswoud, Sharon
Subject: RE: SSI Review: 16 - 0640: OIG Draft Report: IT Management Challenges Continues in TSA's Security Technology Integrated Program

FYI

From (b)(6)
Sent: Tuesday, April 05, 2016 12:26 PM
To: Burke, Kevin
Cc: Twitty, Charles; Huiswoud, Sharon

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

3 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

4 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

Unknown

From: (b)(6)
Sent: Tuesday, April 19, 2016 8:52 AM
To: Huiswoud, Sharon
Cc: Crumpacker, Jim(b)(6)
Subject: RE: Update to Recommendations for Audit Report OIG-15-18

Thank you.

(b)(6)
Audit Liaison
Office of the Chief Information Officer
U.S. Department of Homeland Security
(202) 343(b)(6);(b)(7)(C) Desk)
(202) 253 BlackBerry)

From: Huiswoud, Sharon
Sent: Tuesday, April 19, 2016 8:48 AM
To (b)(6) (b)(6);(b)(7)(C) @hq.dhs.gov> (b)(6) (b)(6);(b)(7)(C) @hq.dhs.gov>
Cc: Crumpacker, Jim (b)(6);(b)(7)(C) @HQ.DHS.GOV>
Subject: FW: Update to Recommendations for Audit Report OIG-15-18

Good Mornin (b)(6)

Attached is a memo from the IG, Mr. Roth regarding open recommendations related to our report, OIG-15-18, *Audit of Security Controls for DHS Information Systems at JFK International Airport.*

Thanks,

Sharon L. Huiswoud
Director
Information Systems and Acquisitions Division
Office of IT Audits
Department of Homeland Security
Office of Inspector General
office: 202-254(b)(6);(b)(7)(
cell: 202-497(b)(6);(b)(7)(

From: Dale, Beverly A.
Sent: Monday, April 18, 2016 4:34 PM
To (b)(6)
Cc: Huiswoud, Sharon; Shappee, Frederick
Subject: Update to Recommendations for Audit Report OIG-15-18

Please distribute.

Requester’s Name: Shawn Musgrave

FOIA/PA NO.: 2015-087

2 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

Unknown

From: DHS-OIG Office of Public Affairs
Sent: Friday, January 09, 2015 11:26 AM
To: Pistole, John; Fulghum, Chip (b)(6);(b)(7)(C) Eisensmith, Jeffrey; (b)(6) (b)(7)(C);(b)(6)
(b)(6);(b)(7)(C) Crumpacker, Jim; (b)(6);(b)(7)(C)
(b)(6);(b)(7)(C) Perkins, Susan (b)(6);(b)(7)(C)
(b)(6);(b)(7)(C)
(b)(6);(b)(7)(C) Crumpacker, Jim; (b)(6) ESEC DHS Reports (b)(6)
(b)(6) GAO-OIG Liaison; (b)(6) (b)(6);(b)(7)(C)
(b)(6);(b)(7)(C)
Cc: Huiswoud, Sharon; Grady, Sharell; Dale, Beverly A.; Shappee, Frederick; Balaban, Dorothy; Hurley, Kim; OIG's DHS Liaison; DHS-OIG Office of Public Affairs; DHS-OIG Office of Legislative Affairs; Manduzio, James; Nadon, Patrick
Subject: OIG-15-18, "Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport-Sensitive Security Information."
Attachments: Security Envelope.pdf; OIG-15-18 Redacted.pdf

Good Morning,

Attached is the final report, OIG-15-18, ***"Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport-Sensitive Security Information."*** The SSI version of this document is password protected and an email containing the password will be forwarded to you shortly.

***This is an advance copy that has not been made public by the DHS OIG. Do Not Distribute Without OIG Authorization.** The projected date for delivery to **Congress is January 15, 2015**. The projected date for **Web posting is January 19, 2015**. Actual dates may differ please contact OIG to confirm.

Thank you,

Office of Public Affairs
Office of Inspector General
Department of Homeland Security
Phone: 202.254.4100
www.oig.dhs.gov l Twitter: @DHSOIG

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

DEC 16 2014

MEMORANDUM FOR: The Honorable Chip Fulghum
Acting Under Secretary for Management

FROM: John Roth John Roth
Inspector General

SUBJECT: *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport*

Attached for your information is our final report, *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport.* This report contains findings and recommendations for improving security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS information technology infrastructure at this airport.

We provided a draft of this report on July 22, 2014, for review. On October 20, 2014, the Departmental GAO-OIG Liaison Office finally conveyed the TSA Sensitive Security Information (SSI) Program Office's response to our request for a sensitivity review by marking several passages in the report as SSI. I disagree with this determination. On November 19, 2014, I sent a formal challenge memo to TSA Administrator John Pistole and copied SSI Program Chief Doug Blair, expressing my disagreement. My challenge is in accordance with procedures outlined in DHS Management Directive MD11056.1. Under this directive, a formal challenge may be submitted, in writing, to the person who made the SSI markings or to the SSI Office.

To date, I have not yet received a response from TSA. I challenged TSA's determination based on the following:

- First, the same or similar information as that marked as SSI in the current draft report was disclosed to the public in previously released DHS OIG and GAO reports. The Department reviewed and approved the content of these previously released reports and did not determine at the time that the information was SSI. See, e.g., *Audit of Security Controls for DHS Information Technology Systems*

at Dallas/Fort Worth International Airport, OIG-14-132 (September 2014).

- Second, even if past reports had not released similar information, its release in this report would not be detrimental to transportation security. For example, the language marked SSI reveals generic vulnerabilities that are common to virtually all systems. In addition, the descriptions of the vulnerabilities are not specific enough to be detrimental. We have published similar findings in reports concerning other DHS components with no detrimental impact. See, e.g., *Implementation Status of EINSTEIN 3 Accelerated*, OIG-14-52 (March 2014).

- Lastly, although the SSI Office marked information in the TSA and CBP Patch Management sections of the draft report as SSI, the SSI Program Office did not mark the same information in another section of the very same report as SSI. Specifically, the ICE section of the draft report includes the same table and wording regarding scanning vulnerabilities as in the TSA and CBP sections. As such, the SSI determination appears to be inconsistently applied.

For these reasons, I have requested that the TSA Administrator reconsider and remove its SSI markings from our draft report. These markings impede the effectiveness and transparency of our office. Per DHS MD 11056.1, section VI.A.3, SSI markings should not be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency. I believe that based on the reasons outlined above, this report should be released in its entirety in the public domain.

The Inspector General Act requires the OIG to conduct audits and investigations that promote the economy, efficiency, and effectiveness of DHS programs and operations, and to keep the Secretary and the Congress fully and timely informed. *The Inspector General Act* also requires the OIG to post its audit reports, or portions thereof, on its website so that the public may easily access the information. Our ability to issue reports that are transparent, without unduly restricting information, is key to accomplishing our mission.

In 2006, Congress, concerned about delays in appeals of this nature, directed the Department to revise MD 11056.1 to require TSA to ensure a timely SSI review of public requests for release of information. Given the

clear requirement in MD 11056.1, for timely SSI reviews in response to requests from the public, we hoped that TSA would approach an SSI appeal from a fellow component with similar diligence, especially since TSA is aware of our deadlines. We are disappointed. Now, to meet our reporting deadline, we are compelled to publish a redacted report with SSI markings we believe are incorrect since we still have not received a timely response to our SSI challenge memorandum.

Congress, when it passed the *Reducing Over-Classification Act* in 2010, found that overclassification "interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information." The Act directed DHS to take steps to guard against over-classification.

Consistent with our responsibilities under the *Inspector General Act*, we will provide unredacted copies of our report to appropriate Congressional Committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted report on our website for public dissemination.

I appreciate your attention to this matter. Should you have any questions, please call me, or your staff may contact Sondra McCauley, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4041.

Attachment

OFFICE OF INSPECTOR GENERAL

Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport (Redacted)

Homeland Security

January 7, 2015
OIG-15-18

HIGHLIGHTS

Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport

January 7, 2015

Why We Did This

We evaluated technical and information security policies and procedures of Department of Homeland Security components at the John F. Kennedy International Airport. Our evaluation focused on how these components have implemented operational, technical, and management controls for computer security at the airport and nearby locations.

What We Recommend

We made recommendations addressing the control deficiencies identified in this report. The information technology security controls implemented at several sites had deficiencies that, if exploited, could have resulted in the loss of confidentiality, integrity, and availability of the components' information technology systems.

What We Found

The Department's information technology security controls implemented at several sites had deficiencies that, if exploited, could have resulted in the loss of confidentiality, integrity, and availability of the components' information technology systems. We identified numerous deficiencies in the information technology security controls associated with the Transportation Security Administration. Additionally, operational environmental controls and security documentation needed improvement. Further, information security vulnerabilities were not resolved timely. Technical security controls for Customs and Border Protection and Immigration and Customs Enforcement information technology resources also needed improvement. The Transportation Security Administration, Customs and Border Protection, and Immigration and Customs Enforcement did not perform required security authorization or privacy reviews on closed–circuit television and surveillance monitoring room technology. The U.S. Secret Service fully complied with DHS sensitive security policies at the airport.

Management Response

We briefed the DHS Chief Information Security Officer and the components on the results of our audit. The draft report included 14 recommendations and DHS concurred with 13 of the 14 recommendations. DHS did not concur with recommendation number six. We do not agree with DHS's response to this recommendation. The response does not provide for corrective actions to address the security and privacy concerns identified in our report. Therefore, we issued two additional recommendations, one for the DHS Chief Information Officer and another for the DHS Chief Privacy Officer.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

DEC 16 2014

MEMORANDUM FOR: The Honorable Chip Fulghum
Acting Under Secretary for Management

FROM: John Roth John Roth
Inspector General

SUBJECT: *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport*

Attached for your information is our final report, *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport.* This report contains findings and recommendations for improving security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS information technology infrastructure at this airport.

We provided a draft of this report on July 22, 2014, for review. On October 20, 2014, the Departmental GAO-OIG Liaison Office finally conveyed the TSA Sensitive Security Information (SSI) Program Office's response to our request for a sensitivity review by marking several passages in the report as SSI. I disagree with this determination. On November 19, 2014, I sent a formal challenge memo to TSA Administrator John Pistole and copied SSI Program Chief Doug Blair, expressing my disagreement. My challenge is in accordance with procedures outlined in DHS Management Directive MD11056.1. Under this directive, a formal challenge may be submitted, in writing, to the person who made the SSI markings or to the SSI Office.

To date, I have not yet received a response from TSA. I challenged TSA's determination based on the following:

- First, the same or similar information as that marked as SSI in the current draft report was disclosed to the public in previously released DHS OIG and GAO reports. The Department reviewed and approved the content of these previously released reports and did not determine at the time that the information was SSI. See, e.g., *Audit of Security Controls for DHS Information Technology Systems*

at Dallas/Fort Worth International Airport, OIG-14-132 (September 2014).

- Second, even if past reports had not released similar information, its release in this report would not be detrimental to transportation security. For example, the language marked SSI reveals generic vulnerabilities that are common to virtually all systems. In addition, the descriptions of the vulnerabilities are not specific enough to be detrimental. We have published similar findings in reports concerning other DHS components with no detrimental impact. See, e.g., *Implementation Status of EINSTEIN 3 Accelerated*, OIG-14-52 (March 2014).

- Lastly, although the SSI Office marked information in the TSA and CBP Patch Management sections of the draft report as SSI, the SSI Program Office did not mark the same information in another section of the very same report as SSI. Specifically, the ICE section of the draft report includes the same table and wording regarding scanning vulnerabilities as in the TSA and CBP sections. As such, the SSI determination appears to be inconsistently applied.

For these reasons, I have requested that the TSA Administrator reconsider and remove its SSI markings from our draft report. These markings impede the effectiveness and transparency of our office. Per DHS MD 11056.1, section VI.A.3, SSI markings should not be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency. I believe that based on the reasons outlined above, this report should be released in its entirety in the public domain.

The Inspector General Act requires the OIG to conduct audits and investigations that promote the economy, efficiency, and effectiveness of DHS programs and operations, and to keep the Secretary and the Congress fully and timely informed. *The Inspector General Act* also requires the OIG to post its audit reports, or portions thereof, on its website so that the public may easily access the information. Our ability to issue reports that are transparent, without unduly restricting information, is key to accomplishing our mission.

In 2006, Congress, concerned about delays in appeals of this nature, directed the Department to revise MD 11056.1 to require TSA to ensure a timely SSI review of public requests for release of information. Given the

clear requirement in MD 11056.1, for timely SSI reviews in response to requests from the public, we hoped that TSA would approach an SSI appeal from a fellow component with similar diligence, especially since TSA is aware of our deadlines. We are disappointed. Now, to meet our reporting deadline, we are compelled to publish a redacted report with SSI markings we believe are incorrect since we still have not received a timely response to our SSI challenge memorandum.

Congress, when it passed the *Reducing Over-Classification Act* in 2010, found that overclassification "interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information." The Act directed DHS to take steps to guard against over-classification.

Consistent with our responsibilities under the *Inspector General Act*, we will provide unredacted copies of our report to appropriate Congressional Committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted report on our website for public dissemination.

I appreciate your attention to this matter. Should you have any questions, please call me, or your staff may contact Sondra McCauley, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4041.

Attachment

Table of Contents

Executive Summary.......... 1

Background 2

Results of Audit.......... 4

TSA Did Not Comply Fully with DHS Sensitive Systems Policies.......... 4
Recommendations 16
Management Comments and OIG Analysis 17

CBP Did Not Comply Fully with DHS Sensitive Systems Policies.......... 20
Recommendations 26
Management Comments and OIG Analysis 27

ICE Did Not Comply Fully with DHS Sensitive Systems Policies.......... 29
Recommendations 33
Management Comments and OIG Analysis 34

USSS Fully Complied with DHS Sensitive Systems Policies.......... 36

Department's Noncurrence.......... 36

Appendixes

Appendix A: Objectives, Scope, and Methodology.......... 37
Appendix B: Management Comments to the Draft Report.......... 39
Appendix C: DHS Activities at JFK Airport.......... 44
Appendix D: Major Contributors to This Report.......... 49
Appendix E: Report Distribution 50

Abbreviations

Airport Authority	Port Authority of New York and New Jersey
CBP	U.S. Customs and Border Protection
CCTV	closed-circuit television
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security

FAMS	Federal Air Marshall Service
FAMSNet	Federal Air Marshall Service Network
GAO	Government Accountablity Office
ICE	U.S. Immigration and Customs Enforcement
IT	information technology
JFK	John F. Kennedy International Airport
OIG	Office of Inspector General
OMB	Office of Management and Budget
OneNet	DHS One Network
PIA	privacy impact assessment
PII	personally identifiable information
PTA	privacy threshold assessment
Security System	Airport Authority Selected Surveillance Systems
TECS	Treasury Enforcement Communication System
TSA	Transportation Security Administration
TSANet	Transportation Security Administration Network
UPS	uninterruptible power supply
USSS	United States Secret Service

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Executive Summary

As part of our Technical Security Evaluation Program, we evaluated technical and information security policies and procedures of Department of Homeland Security components at the John F. Kennedy International Airport. Four Department components – the Transportation Security Administration, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Secret Service – operate information technology systems that support homeland security operations at this major airport.

Our evaluation focused on how these components have implemented operational, technical, and management controls for computer security at the airport and nearby locations. We performed onsite inspections of the areas where these assets were located, interviewed departmental staff, and conducted technical tests of computer security controls. We also reviewed applicable policies, procedures, and other relevant documentation.

The Department's sensitive system security policies, the information technology security controls implemented at several sites had deficiencies that, if exploited, could have resulted in the loss of confidentiality, integrity, and availability of the components' information technology systems. We identified numerous deficiencies in the information technology security controls associated with the Transportation Security Administration. Additionally, operational environmental controls and security documentation needed improvement. Further, information security vulnerabilities were not resolved timely. Technical security controls for Customs and Border Protection and Immigration and Customs Enforcement information technology resources also needed improvement. The Transportation Security Administration, Customs and Border Protection, and Immigration and Customs Enforcement did not perform required security authorization or privacy reviews on closed–circuit television and surveillance monitoring room technology. The U.S. Secret Service fully complied with DHS sensitive security policies at the airport.

The draft report included 14 recommendations and DHS concurred with 13 of the 14 recommendations. DHS did not concur with recommendation number six. We do not agree with DHS's response to this recommendation, as it does not provide for corrective actions to address the security and privacy concerns identified in our report. To help ensure that these security and privacy concerns get addressed properly, we issued two additional recommendations for the DHS Chief Information Officer and DHS Chief Privacy Officer. We have included a copy of the Department's comments to the draft report in their entirety in appendix B.

Background

We designed our Technical Security Evaluation Program to provide senior Department of Homeland Security officials with timely information on whether they had properly implemented DHS information technology (IT) security policies at critical sites. Our program audit was based on the requirements identified within *DHS Sensitive Systems Policy Directive 4300A,* version 10.0, which provides direction to DHS component managers and senior executives regarding the management and protection of sensitive systems. This directive and an associated handbook outline policies on the operational, technical, and management controls necessary to ensure confidentiality, integrity, and availability within the DHS IT infrastructure and operations. These controls are as follows:

- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people to improve system security. For example, operational control mechanisms include physical access controls that restrict the entry and exit of personnel from an area, such as an office building, data center, or room, where sensitive information is accessed, stored, or processed.

- **Technical Controls** – Focus on security controls executed by information systems. These controls provide automated protection from unauthorized access; facilitate detection of security violations; and support applications and data security requirements. For example, technical controls include passwords for systems.

- **Management Controls** – Focus on managing both the system information security controls and system risk. These controls include risk assessments, rules of behavior, and ensuring that security is an integral part of both system development and IT procurement processes.

We evaluated security controls for IT systems that support homeland security operations of the Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Secret Service (USSS) at John F. Kennedy International Airport (JFK). Figure 1 shows Terminal Four at JFK.

Figure 1-JFK Terminal Four

JFK is the sixth busiest airport in the United States. With arrivals and departures from almost every international airline in the world, JFK is an international gateway for passengers and heavy freight. Below are some facts about JFK.

- JFK, on the Jamaica Bay in New York City, is a designated port of entry.[1] The airport covers over 4,930 acres, including 30 miles of roadway. JFK has 6 operating airline terminals and more than 125 airline gates.

- Port Authority of New York and New Jersey (Airport Authority) operates JFK under a lease with the City of New York since 1947, with the current lease continuing until 2050. The Airport Authority has invested over $10 billion in the airport.

- JFK contributes about $30.6 billion in economic activity annually to the New York/New Jersey region, generating approximately $4.2 billion in direct wages; 71,000 jobs and indirect wages of $30.5 billion for 213,400 jobs.

- JFK is a leading international air cargo center. This facility has more than four million square feet of office and warehouse space dedicated to cargo operations serving the New York and New Jersey region. The entire air cargo area has automated and computer-controlled terminals containing one or more restricted access sites.

[1] Port of entry is defined as a designated controlled entry points into the United States from foreign countries.

See appendix C for specific details of DHS component activities at the JFK airport.

Results of Audit

TSA Did Not Comply Fully with DHS Sensitive Systems Policies

TSA did not comply fully with DHS operational, technical, and management policies for its servers and switches operating at JFK. Specifically, physical security and access controls for numerous TSA server rooms and communication closets were deficient. Additionally, TSA had not implemented known software patches to its servers at JFK. Finally, TSA did not designate the closed-circuit television (CCTV) cameras as a DHS IT system nor did it implement the applicable, operational, technical, and managerial controls for the cameras. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability, of the data stored, transmitted, and processed by TSA at JFK.

Operational Controls

We evaluated TSA server rooms and communication closets containing IT assets at JFK. We identified operational controls that did not conform fully to DHS policies. Specifically, we identified deficiencies in physical security, visitor logs, the fire protection system, storage and housekeeping, electronic power supply protection, and humidity and temperature controls.

Physical Security

Adequate access controls have not been established limiting access to TSA sensitive equipment in JFK terminals. [redacted]

[redacted]

The door to the secure Explosive Detection Systems room, where TSA reviews x-ray images of luggage to determine if suspicious checked luggage requires additional inspection, was propped open to vent a portable air conditioning unit, violating physical security controls. Figures 3a, 3b, and 3c show the required access control into the room, a secondary door to the room left open, and an air conditioning unit venting hot air out through the open door.

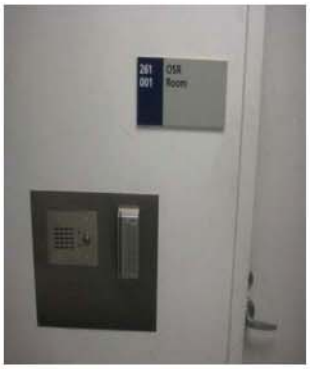


Figure 3a-Access Control

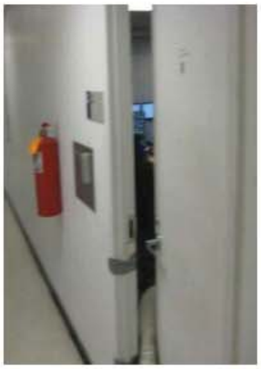


Figure 3b-Unsecured Door

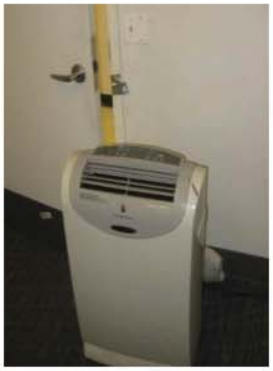


Figure 3c-Climate Control

According to DHS Sensitive System Policy Directive 4300A:

> Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.

Physical security vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of TSA data. Unauthorized access to TSA server rooms may result in the loss of IT processing capability used for passenger and baggage screening.

Visitor Logs

At JFK, TSA did not have visitor logs in any of its communication rooms to document the entry and exit of visitors to these rooms that contain sensitive IT equipment.

According to DHS Sensitive System Policy Directive 4300A:

> Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data. They shall be escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.

When unauthorized individuals gain access to locations where sensitive computing resources reside, there is an increased risk of system compromise and data confidentiality, integrity, and availability concerns.

Fire Protection System

Fire protection, detection, and suppression controls were not present in many TSA communication rooms. Specifically, 14 of the 21 rooms inspected that contained sensitive equipment did not have fire extinguishers. Additionally, 8 of the 21 rooms did not have a fire suppression system installed. As a result, 5 rooms were in violation of fire protection policy. Table 1 shows the existence or lack of fire protection equipment at the locations inspected.

Table 1-TSA Fire Protection

TSA Fire Protection			
Identification of the room	**Smoke Detector**	**Fire Extinguisher**	**Fire Suppression**
TSA Location 1	Yes	No	Yes
TSA Location 2	Yes	No	Yes
TSA Location 3, TSA/FAMS	No	No	Yes
TSA Location 4, Terminal 1	No	No	No
TSA Location 5, Terminal 1	No	No	Yes
TSA Location 6 Terminal 1	Yes	No	Yes
TSA Location 7, Terminal 2	No	No	Yes
TSA Location 8, Terminal 4	No	No	Yes
TSA Location 9, Terminal 4	Yes	Yes	No
TSA Location 10, Terminal 4	No	No	No
TSA Location 11, Terminal 4	Yes	Yes	No
TSA Location 12, Terminal 5	No	No	Yes
TSA Location 13, Terminal 5	Yes	No	Yes
TSA Location 14, Terminal 5	No	Yes	Yes
TSA Location 15, Terminal 7	No	No	No
TSA Location 16, Terminal 7	No	Yes	No
TSA Location 17, Terminal 7	No	No	No
TSA Location 18, Terminal 7	No	No	No
TSA Location 19, Terminal 8	Yes	Yes	Yes
TSA Location 20, Terminal 8	No	Yes	Yes
TSA Location 21, Terminal 8	No	Yes	Yes

According to DHS 4300A Sensitive Systems Handbook:

> Fire protection systems should be serviced by professionals on a recurring basis to ensure that the systems stay in proper working order. The following should be considered when developing a fire protection strategy:
>
> - When a centralized fire suppression system is not available, fire extinguishers should be readily available.
> - Facilities should make available/provide Class C fire extinguishers, designed for use with electrical fire and other types of fire.
> - Fire extinguishers should be located in such a way that a user would not need to travel more than 50 feet to retrieve one.

Compounding the issue of fire detection and mitigation, only 7 of 21 the rooms inspected contained smoke detectors. Smoke detectors alert the appropriate personnel of a potential fire and possible hazard.

The DHS 4300A Sensitive Systems Handbook also states:

> In addition to the physical security controls discussed above, facility managers and security administrators must also ensure that environmental controls are established, documented, and implemented to provide needed protection in the following areas:
>
> - Fire protection, detection, and suppression

In addition to DHS 4300A Sensitive Systems Handbook, TSA's Information Assurance Handbook states:

> The Facility Security manager shall employ and maintain fire suppression and detection devices/systems (to include sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors) for the TSA facility information systems that are supported by an independent energy source. When centralized fire suppression is not available, Class C fire extinguishers should be readily available. Each class C fire extinguisher

should be located in such a way that the user would not need to travel more than 50 feet to retrieve it.

The lack of fire notification capabilities and unmitigated suppression system vulnerabilities place at risk the availability of TSA data. For example, sensitive equipment damaged by fire may not be available for TSA's passenger and baggage screening processes.

Storage and Housekeeping

Several TSA communication closets located in the JFK terminals contained storage items and cleaning supplies. For example, we found TSA equipment on top of an unlocked TSA telecommunication cabinet surrounded by a ladder, boxes, trash, and cleaning supplies. The ladder, boxes, and cleaning supplies are all harmful to IT equipment. Additionally, there was no sign in sheet, and non-TSA personnel used the room for equipment storage. Figures 4 and 5, show cleaning supplies and maintenance equipment stored with TSA IT hardware in a communication room and communication closet.

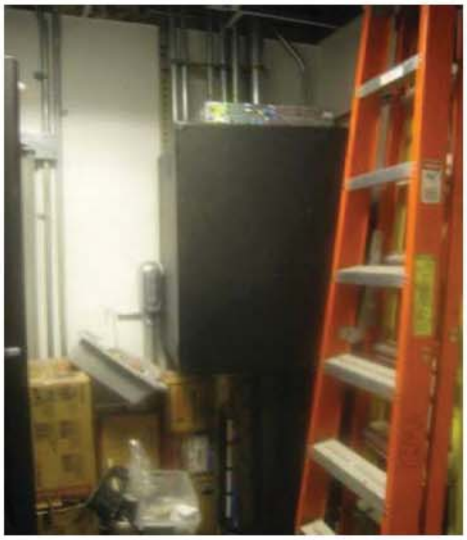


**Figure 4 -
Unlocked Communication Cabinet with Unsecured TSA Equipment**

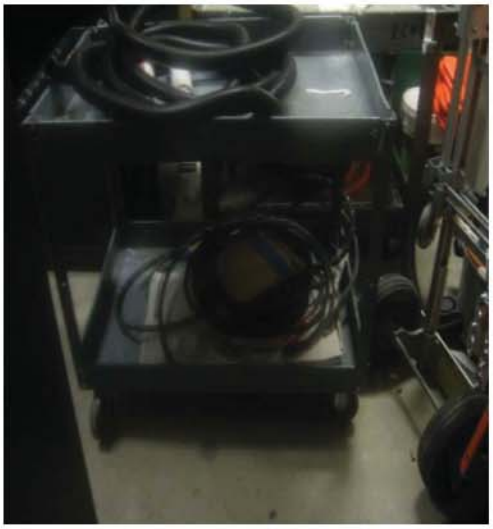


**Figure 5 -
Communication Room used as Storage**

Items being stored in the room were an obstruction and preventing access to the TSA IT equipment cabinets. A lack of housekeeping and maintenance caused a buildup of dust on TSA IT hardware stored within cabinets as shown in figure 6.

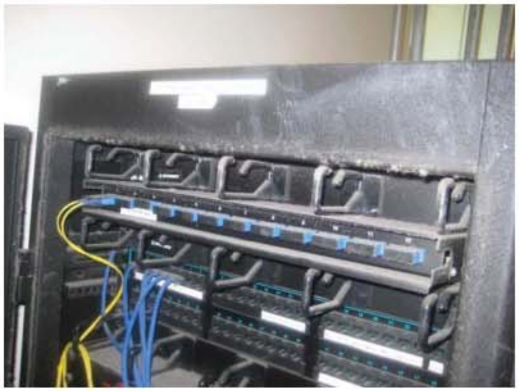


Figure 6- Dust covered Sensitive Equipment

According to DHS 4300A Sensitive Systems Handbook:

- Dusting of hardware and vacuuming of work area should be performed weekly with trash removal performed daily. Dust accumulation inside of monitors and computers is a hazard that can damage computer hardware.
- Cleaning supplies should not be stored inside the computer room.

Storage and housekeeping issues place the availability of TSA data at risk. Computer hardware damaged by dust and debris has the potential to cause delays for TSA's passenger and baggage screening processes.

Electronic Power Supply Protection

TSA did not have an operable uninterruptible power supply (UPS) in three communication cabinets. Figure 7 shows an unlocked cabinet and figure 8 shows inoperable UPS equipment.

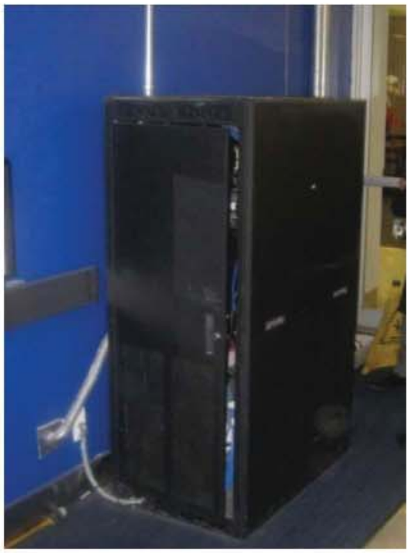


Figure 7-
Accessible Equipment

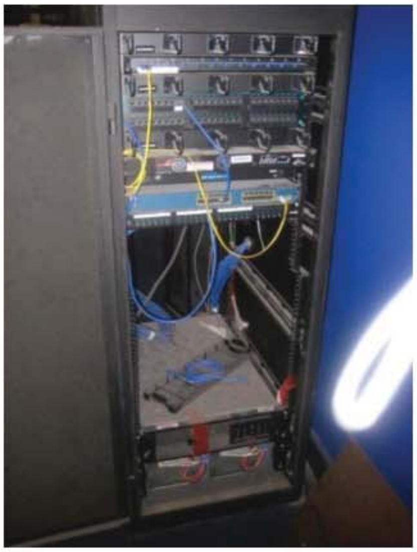


Figure 8-
Inoperable UPS

A sensitive equipment cabinet located in a public area was unlocked and left open to run an extension cord to a nearby electrical outlet for power. Upon closer inspection, we determined that the UPS was inoperable and not being used to provide backup power to IT equipment. Additionally, the attached extension cord prohibited the cabinet from closing and locking.

According to the *DHS 4300A Sensitive Systems Handbook*:

> Electrical power must be filtered through an UPS system for all servers and critical workstations and surge suppressing power strips used to protect all other computer equipment from power surges.

Electrical power supply vulnerabilities place TSA data availability at risk. For example, TSA servers that are not connected to a working UPS may not operate following a power outage.

Humidity and Temperature Controls

TSA did not have any device to measure humidity in the 21 server/switch rooms that we visited at JFK. Additionally, 13 out of the 21 server/switch rooms did not contain temperature sensors. Of the eight rooms that had temperature sensors, only two had temperature readings within the acceptable range established by DHS policy.

According to the *DHS 4300A Sensitive Systems Handbook*:

- Humidity should be at a level between 35 percent and 65 percent.
- Temperatures in computer storage areas should be between 60 and 70 degrees Fahrenheit.

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Technical Controls

TSA's implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, identified vulnerabilities on TSA servers at JFK had not been resolved or patched in a timely fashion.

Patch Management

In February 2014, we observed TSA staff scan two servers located at JFK for vulnerabilities. [redacted][2] Table 2 provides the number of vulnerabilities by server.

[2] Critical vulnerabilities should be addressed immediately due to the imminent threat to a network.

Table 2- Critical, High, and Medium Vulnerabilities

TSA Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]

According to *DHS Sensitive Systems Policy Directive 4300A*:

> Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.

Server vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of TSA data.

Management Controls

TSA's implementation of management controls for the Airport Authority's Security Systems operating at JFK did not conform fully to DHS policies. Specifically, TSA had not designated the Security System as a DHS IT system. As a result, TSA had not performed the applicable security authorization processes and privacy requirements over the surveillance system at JFK terminals.

CCTVs and Surveillance Systems

TSA did not designate the JFK CCTV cameras and surveillance system as DHS IT systems. As a result, the component did not implement the applicable, operational, technical, and managerial controls for the cameras and the systems. TSA officials stated that it was not responsible for the cameras and surveillance system because they belong to the Airport Authority.

However, TSA provided the funding for the JFK CCTV cameras and surveillance systems to the New York Airport Authority. The funding was an estimated $7.2 million to design, install, and maintain the JFK CCTV intrusion detection systems and other surveillance equipment. The Airport Authority Selected Surveillance Systems (Security System) includes CCTV cameras, detection systems, other surveillance hardware, storage equipment, and associated electrical cabling, and

support facilities monitored at JFK. The Airport Authority sets the conditions for shared use of these systems throughout JFK. Figure 9 shows the TSA's Security System.

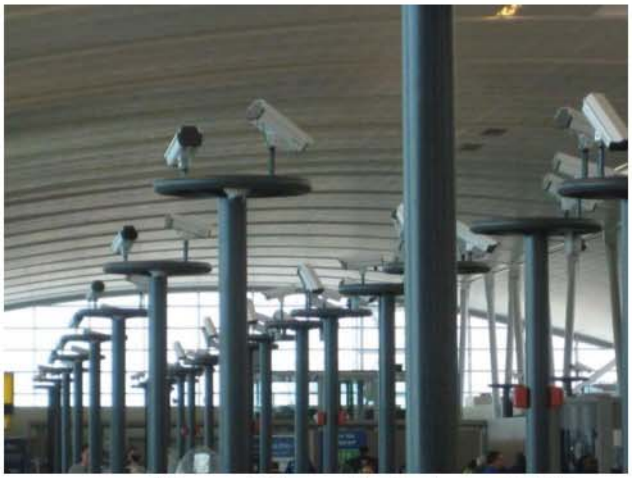


Figure 9-Security System at JFK

According to the agreement between the Airport Authority and TSA, the Security System provides greater surveillance of TSA areas to enhance security at JFK and assists in resolution of law enforcement issues. The Airport Authority is the owner of the Security System and is responsible for the repairs and maintenance. All media generated from the Security System remains with the Airport Authority. Although, the Airport Authority owns the systems, TSA controls the system design, identification of milestones, and who has allowable access to the system data. TSA officials also have unlimited ability to access information from the Security System to conduct TSA administrative or Top Secret criminal investigations.

The Security System collects images from all cameras to a video management system that stores the information for a minimum of 31 days. Since information that DHS uses is being stored, transmitted, and monitored on this system, and the Port Authority is operating this system on behalf of TSA, then TSA has the requirement to designate the Security System as a DHS IT system. However, TSA officials stated that because this system belongs to the Airport Authority it did

not need to conduct required security authorization processes, a privacy threshold analysis (PTA), or a privacy impact assessment (PIA).[3]

According to *DHS Sensitive Systems Policy Directive 4300A*:

> A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf.

DHS Sensitive Systems Policy Directive 4300A states that Component Chief Information Security Officers (CISO) shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

[3] A privacy threshold analysis is performed to determine if additional privacy compliance documentation is required, such as a privacy impact assessment. A privacy impact assessment is a publicly released assessment of the privacy impact of an information system and includes an analysis of the personally identified information collected, stored, and shared.

PII includes photographic facial images and any other unique identifying number or characteristic.

Also, Office of Management and Budget (OMB) M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when it uses IT to collect new information.

TSA has not fulfilled security authorization or privacy requirements for the cameras and surveillance systems at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put this information at risk, and lead to violations of U.S. privacy laws and DHS policy.

Recommendations

We recommend that the TSA Chief Information Officer (CIO):

Recommendation #1:

Comply with DHS policy concerning physical security, housekeeping and electronic power supply protection at all locations at JFK that contain TSA IT assets.

Recommendation #2:

Comply with DHS policy concerning fire protection at all locations at JFK that contain TSA IT assets.

Recommendation # 3:

Maintain JFK servers and network rooms free of excess storage that may cause damage to the equipment.

Recommendation #4:

Obtain humidity and temperature sensors for the JFK server rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Recommendation #5:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #6:

Designate the intrusion detection and surveillance Security Systems as DHS IT systems and implement applicable management, technical, operational, and privacy controls and reviews.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Assistant Director, Departmental Government Accountability Office (GAO) OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #1 through #5, but non-concurred with recommendation #6. Additionally, TSA has already taken actions and has submitted supporting documentation to resolve the reported deficiencies for recommendations #1, #3, and #5. We consider these recommendations resolved, but open pending verification of corrective and planned actions and supportive documentation.

Recommendation #1:

DHS concurred with recommendation 1. TSA officials recognize the need to comply with DHS policies on physical security, housekeeping, and electrical power supply protection by conducting quarterly cleaning of all IT equipment cabinets as well as ensuring that all uninterrupted power supplies are operational. TSA took several corrective actions and submitted supporting documentation. We agree that the steps TSA is taking, and plans to take, will satisfy this recommendation. Our recommendation will remain open and resolved until we receive and review supporting documentation for the corrective actions.

Recommendation #2:

DHS concurred with recommendation 2. TSA offficals recognize the need to comply with the DHS policy concerning fire protection. TSA plans to take corrective actions to ensure that all locations at JFK that contain TSA IT assets are equipped with fire extinguishers. Additionally, TSA plans to verify the presence of other required fire protection equipment at all of its locations at JFK. TSA estimated that corrective actions would be completed by November 30, 2014.

We agree that the steps that TSA is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until we receive and review the corrective actions and supporting documentation.

Recommendation #3:

DHS concurred with recommendation 3. TSA's response outlines corrective actions for the removal of the excess items and the assurance to refrain from using IT equipment rooms as storage areas. We agree that the steps TSA is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until we receive and review the corrective actions and supporting documentation.

Recommendation #4:

DHS concurred with recommendation 4. TSA recognizes that temperature and humidity levels in computer storage areas should be between 60 and 70 degrees Fahrenheit and at a level between 35 percent and 65 percent, respectively. TSA plans to coordinate with facilities management to ensure that the Airport Authority complies with these requirements. TSA estimated that the corrective actions would be completed by October 31, 2014. We recognize these actions as positive steps and look forward to learning more about the continued progress in the future. This recommendation will remain open and resolved pending receipt and verification of planned actions and supporting documentation

Recommendation #5:

DHS concurred with recommendation 5. TSA stated that it remediated the identified vulnerabilities. TSA also stated that another subsequent security scan of the JFK servers was conducted to ensure vulnerabilities identified previously were no longer present on the servers. TSA provided supporting documentation for this recommendation. This recommendation will remain open and resolved pending verification of corrective actions and supporting documentation.

Recommendation #6:

DHS did not concur with recommendation 6. Instead of addressing directly our recommendation to designate detection and surveillance systems as DHS IT systems and to initiate appropriate IT security and privacy controls, TSA indicated it does not have a relationship at the JFK Airport that meets the definition of DHS 4300A Sensitive Systems Handbook for DHS IT systems. In TSA's

response, it stated that, because the intrusion detection and surveillance security systems are owned and operated by the Airport Authority, it had no responsibility to ensure that IT security and privacy controls were met.

According to the DHS Sensitive Systems Policy Directive 4300A, however, a DHS IT system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf. The systems at JFK transmit, store, and process data on behalf of DHS. Based on the Department's definition, these systems are IT systems and need to be treated as such by DHS. Because TSA has refused to define the detection and surveillance systems as DHS IT systems, TSA did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

We do not agree with DHS's response to this recommendation. The response does not provide for corrective actions to address the security and privacy concerns identified. DHS needs to perform security and privacy reviews of the surveillance systems at JFK airport. By not peforming these reviews, vulnerabilitilies may exist that may put the information collected at risk and lead to security breaches, and violations of DHS policy, and U.S. privacy laws. To assist in this process, we have added additional recommendations, #15 and #16, to our report that will need to be addressed before we can resolve the status of this recommendation.

We look forward to reviewing TSA's progress in the future. However, this recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

CBP Did Not Comply Fully with DHS Sensitive Systems Policies

CBP did not comply fully with DHS operational, technical, and management controls. Specifically, several CBP servers and telecommunication rooms did not contain humidity and temperatures sensors. Additionally, the temperature of several of the rooms reviewed with sensors had room temperatures that exceeded temperature ranges established by DHS policy. The humidity control readings for these rooms were within the ranges set by DHS policy. Also, CBP had an unlocked and open switch device in an open storage area allowing the potential for unauthorized access. In addition, CBP had not implemented known information security software patches to its servers at JFK. Finally, CBP did not designate the CCTV cameras and surveillance room as DHS IT systems nor did they implement the applicable, operational, technical, and managerial controls for these JFK systems. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by CBP at JFK.

Operational Controls

CBP server rooms and communication closets at JFK were clean and well maintained. However, onsite implementation of operational controls did not conform fully to DHS policies. For example, temperatures in CBP JFK server rooms were not within the temperature range recommended by the DHS 4300A Sensitive Systems Handbook. Additionally, one of the CBP sites did not have adequate equipment to prevent unauthorized access to CBP communication switches.

Humidity and Temperature Controls

Six out of 21 CBP switch rooms at JFK did not have humidity and temperature sensors. Five rooms with sensors had temperatures that exceeded temperature ranges established by DHS policy. The humidity control readings for these five rooms were within the ranges set by DHS policy.

According to the *DHS 4300A Sensitive Systems Handbook*:

- Humidity should be at a level between 35 percent and 65 percent.
- Temperatures in computer storage areas should be between 60 and 70 degrees Fahrenheit.

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Inadequate Equipment

CBP did not have a large enough box in the office storage area to contain one of its telecommunication switches. As a result, the box could not properly close. Figure 10 shows the box and the telecommunication switches mounted unprotected, beside the box.

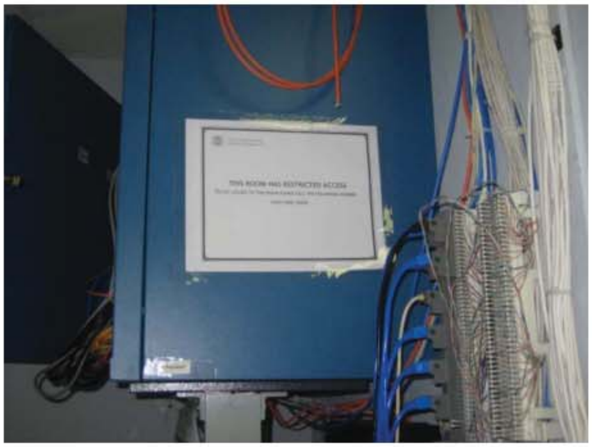


Figure 10- Unlocked Switch Box

According to DHS Sensitive System Policy Directive 4300A:

> Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.

Without adequate physical security controls, unauthorized individuals may gain access to sensitive TSA hardware.

Technical Controls

CBP's implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, identified vulnerabilities on CBP servers were not being resolved in a timely manner.

Patch Management

In February 2014, we observed CBP staff perform vulnerability scans on the three servers located at JFK. [redacted] Table 3 provides the number of vulnerabilities identified by server.

Table 3- Critical, High, and Medium Vulnerabilities

CBP Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]

According to the *DHS 4300A Sensitive Systems Handbook*:

> Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction stated in the Information Security Vulnerability Management message published by the DHS Security Operations Center.

Server vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of CBP data. CBP IT Security officials reviewed the technical results for the three servers and immediately began corrective actions to resolve the two critical vulnerabilities.

Management Controls

CBP's implementation of management controls for the CCTV cameras and surveillance room systems operating at JFK did not conform fully to DHS policies. For example, CBP had not designated the CCTV cameras and surveillance room systems as DHS IT systems. As a result, CBP had not performed the security authorization processes and privacy requirements over the newly installed physical security measures at JFK terminals.

CCTV Cameras and Surveillance Room

CBP did not designate the JFK CCTV cameras and surveillance monitoring room systems as DHS IT systems nor did it implement the applicable, operational, technical, and managerial controls for these JFK systems. CBP failed to designate the cameras and surveillance monitoring room equipment as DHS IT systems, as required by *DHS Sensitive Systems Policy Directive 4300A,* sections 1.4.7 and 1.4.8.

We observed several CCTV cameras in the Terminal 4 area of the CBP passenger processing primary and secondary locations.[4] Figure 11 shows CBP's primary passenger processing area.

[4] Primary processing is the first point of examination of passengers by a CBP officer. Those passengers selected for further examination are referred to a secondary processing point for a more thorough inspection.

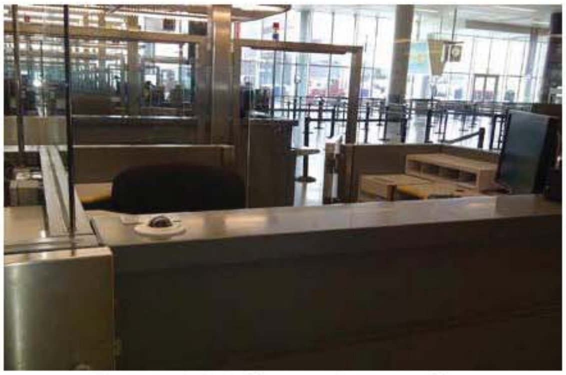


Figure 11-Primary Processing

In 2013, CBP acquired newly renovated space at JFK that included CCTV cameras and a CBP surveillance monitoring room containing IT equipment. The CBP Command and Control Center employees use the cameras to assess threats signaled by alarm events and for surveillance by CBP airport security to monitor activity both inside and outside the terminal.[5] CBP requires a secondary CCTV system that allows officers to monitor detainees in the secondary processing areas, interview rooms, holding rooms, and expedited voluntary removal rooms. CBP officials estimate that approximately 300 cameras are throughout viewable areas within CBP primary passenger processing, secondary passenger processing, interview rooms, and holding rooms. CBP officials operate and monitor the cameras from a CBP secured surveillance monitoring room. Only CBP officials have permission to view cameras observing operations in secondary processing areas. Figure 12 shows the CBP surveillance monitoring room.

[5] Command and Control Center is a station centrally located within the airport's Federal Inspection Service Areas, where CBP systems are monitored.

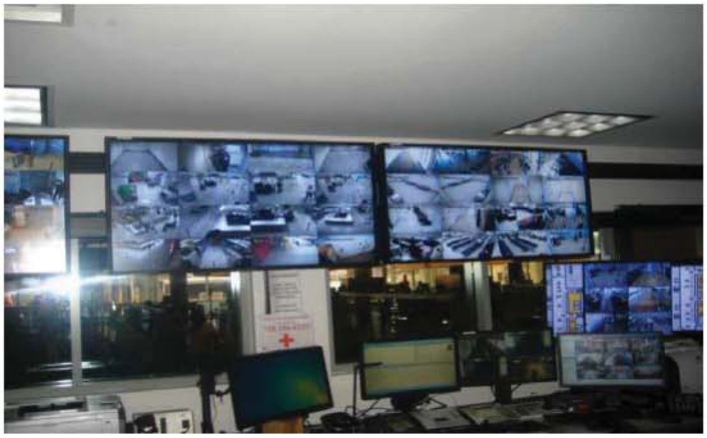


Figure 12- Views of CBP Surveillance Monitoring

The cameras record audio and visual interactions between CBP officers and passengers. However, the Airport Authority owns the CCTV cameras. Since CBP information is being stored, transmitted, and monitored on this system, CBP has the requirement to designate the cameras and surveillance monitoring room as DHS IT systems. By not designating the cameras and surveillance monitoring room as an IT system, CBP did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A.

According to *DHS Sensitive Systems Policy Directive 4300A*:

> A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf.

DHS Sensitive Systems Policy Directive 4300A states that the CISO shall ensure that all information systems are formally assessed through a comprehensive evaluation of management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates PII. Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The

PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

PII includes photographic facial images and any other unique identifying number or characteristic.

Among other things, OMB M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when it uses IT to collect new information.

CBP has not fulfilled security authorization or privacy requirements for the cameras and surveillance equipment at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put the information at risk, and may lead to violations of U.S. privacy laws and DHS policy.

Recommendations:

We recommend that the CBP CIO

Recommendation #7:

Maintain the temperatures of servers and switch rooms within the established temperature ranges.

Recommendation #8:

Secure CBP information technology equipment from unauthorized access.

Recommendation #9:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #10:

Designate the surveillance systems as CBP/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS GAO OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #7 through #10 and has provided details on corrective actions to address each recommendation. We consider these recommendations resolved, but open pending verification of planned actions and supportive documentation.

Recommendation #7:

DHS concurred with recommendation 7. CBP's response outlines its plans to install humidity and temperatures sensors. CBP agrees to set humidity and temperatures to the recommended range per the DHS 4300A Sensitive Systems Handbook. These corrective actions are expected to be completed by December 31, 2014. We believe that such efforts are good steps toward addressing our recommendation. We look forward to receiving additional documentation on CBP's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #8:

DHS concurred with recommendation 8. CBP's response outlines its plans to obtain a lockable rack large enough to secure the identified telecommunication switch from unauthorized access. This corrective action is expected to be completed by January 31, 2015. We look forward to receiving notification from CBP that the lockable rack has been installed and in use. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #9:

DHS concurred with recommendation 9. CBP officials plan to review the OIG reported vulnerabilities to ensure that all critical and high vulnerabilities are addressed. CBP's review is expected to be completed by February 28, 2015. Although, this response appears to address critical and high vulnerabilities, it does not address any corrective actions for the remaining vulnerabilities identified in our report. We look forward to learning more about CBP's actions on this recommendation in the near future. This recommendation will remain open and unresolved pending verification of corrective actions and supporting documentation for all vulnerabilities identified.

Recommendation #10:

Although DHS concurred with recommendation 10, it does not appear that its concurrence addressed all of the concerns noted in our recommendation. Specifically, CBP does not take full ownership of all of the CCTV cameras. CBP agrees that it needs to perform a PTA for CBP's collection and use of the CCTV information. Additionally, CBP plans to determine whether further privacy compliance coverage is warranted through an update to DHS/CBP's current CCTV PIA.

However, CBP only plans to perform the PTA and PIA on the cameras it owns. Although the Port Authority owns some of the cameras in CBP's areas, these cameras and surveillance systems also store, transmit, and monitor CBP information. As a result, CBP has the requirement to designate the cameras and surveillance monitoring room systems as DHS IT systems and to perform required security and privacy reviews. By not designating the cameras and surveillance monitoring room systems as a DHS IT system, CBP did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

DHS/CBP did not provide sufficient corrective actions for our review. We look forward to reviewing CBP's progress in the future. However, this recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

ICE Did Not Comply Fully with DHS Sensitive Systems Policies

ICE did not comply fully with DHS operational, technical and management policies for its servers and switches operating at JFK. Specifically, ICE server and telecommunication rooms did not contain humidity and temperature sensors. Also, ICE had not implemented identified information security patches to its servers. Additionally, ICE did not designate the CCTV cameras and surveillance monitoring equipment as DHS IT systems nor did it implement the applicable, operational, technical, and managerial controls for these JFK systems. Finally, ICE CCTV cameras and surveillance system did not function properly or reliably. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by ICE at JFK.

Operational Controls

ICE server rooms and communications closets at JFK were clean and well maintained. However, onsite implementation of operations controls did not conform fully to DHS policies. For example, the ICE servers and switch rooms did not have the appropriate humidity and temperature control devices to measure and record humidity and temperature ranges as required by DHS policies.

Humidity and Temperature Controls

The ICE servers and switch rooms did not contain any humidity and temperature sensors.

According to the *DHS 4300A Sensitive Systems Handbook*:

- Humidity should be at a level between 35 percent and 65 percent.
- Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit.

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Technical Controls

Patch Management

ICE implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, vulnerabilities identified on ICE servers were not being resolved in a timely fashion. Table 4 provides the number of critical, high, and medium level vulnerabilities identified for each server.

Table 4- Critical, High, and Medium Vulnerabilities

ICE Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	0	1	6
2	0	2	4
3	0	0	2
4	0	1	2
Total	0	4	14

According to the DHS 4300A Sensitive Systems Handbook:

> Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction as stated in the Information Security Vulnerability Management message published by the DHS Security Operations Center.

Server vulnerabilities that are not mitigated could compromise the confidentiality, integrity, and availability of ICE data. If the identified security vulnerabilities are not addressed, they could lead to the introduction of malicious code or unauthorized access to ICE information systems.

Management Controls

CCTV and Surveillance Systems

ICE's implementation of management controls over its CCTV cameras and surveillance systems for the physical security requirements at JFK did not conform fully to DHS policies. Specifically, in April 2010, ICE acquired space at Terminal 4, JFK for the Joint Narcotics and Smuggling Unit. This space includes CCTV cameras, a surveillance monitor, and a digital video receiver. Figure 13 shows the ICE surveillance monitor.

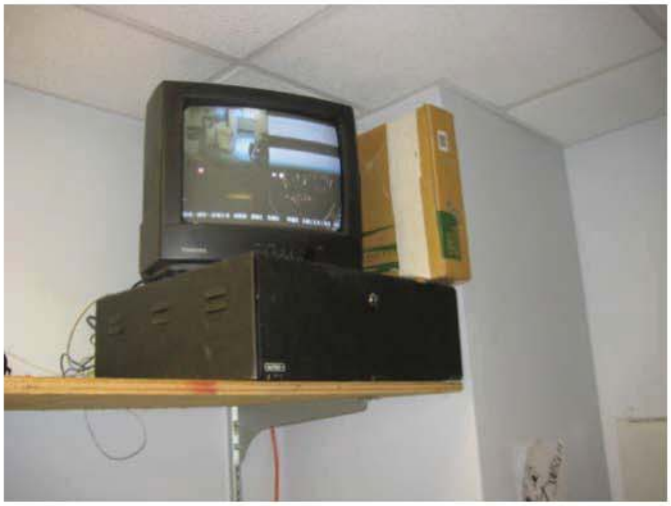


Figure 13- ICE's Surveillance Monitor

However, ICE failed to designate the cameras and surveillance monitor as a DHS IT system as required by *DHS Sensitive Systems Policy Directive 4300A,* sections 1.4.7 and 1.4.8.

ICE officials stated that they did not designate the cameras and surveillance monitor as a DHS IT system because the Airport Authority owned the system. Since ICE information is being stored, transmitted, and monitored on this system, then ICE has the requirement to designate the cameras and surveillance monitor as a DHS IT system. By not designating the cameras and surveillance monitoring room systems as a DHS IT system, ICE did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming

these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

Additionally, two of four CCTV cameras at the Terminal 4 Joint Narcotics and Smuggling Unit communication room were not working during our site visit. The surveillance system monitor connected to the CCTV cameras did not properly display all captured images. ICE officials stated that the cameras had not worked for a period of time but the surveillance system monitor was operating properly 3 days prior to our visit. The ICE officials indicated that they would request camera repairs.

According to *DHS Sensitive Systems Policy Directive 4300A*:

> A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf.

DHS Sensitive Systems Policy Directive 4300A states that the CISO shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates PII. Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

PII includes photographic facial images and any other unique identifying number or characteristic.

Also, OMB M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when they use IT to collect new information.

ICE has not fulfilled security authorization or privacy requirements for the cameras and surveillance equipment at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put the information at risk, and lead to violations of U.S. privacy laws and DHS policy.

Lastly, the identified vulnerabilities on ICE CCTV cameras and surveillance monitor degrade physical security for ICE and law enforcement staff members.

Recommendations

We recommend that the ICE CIO:

Recommendation #11:

Obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Recommendation #12:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #13:

Designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Recommendation #14:

Upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit at JFK.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS GAO OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #11 through #14 and has already taken actions to resolve reported deficiencies. We consider these recommendations resolved, and open pending verification of planned actions.

Recommendation #11:

DHS concurred with recommendation 11. The ICE OCIO plans to to obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300A Sensitive Systems Handbook. ICE estimated the corrective actions would be completed by October 31, 2014. We look forward to receiving additional documentation on ICE's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #12:

DHS concurred with recommendation 12. The ICE OCIO plans to remediate vulnerabilities as they are identified, or within timeframes specified by the DHS Security Operations Center messages. ICE expects this process to be an ongoing effort, however, with an estimated completion date of December 31, 2014. We look forward to receiving additional documentation on ICE's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #13:

DHS concurred with recommendation 13. ICE agreed with the intent of this recommendation for the the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ICE's OCIO and Homeland Security Investigations plans to coordinate and designate the surveillance systems as ICE/DHS IT systems. ICE also plans to implement applicable DHS management, technical, operational controls, and privacy controls and reviews. ICE anticipates completing corrective actions for this recommendation by June 30, 2015. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #14:

DHS concurred with recommendation 14. ICE's Homeland Security Investigations, with assistance from the ICE OCIO, plans to assess the feasibility to upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ICE officials estimate the completion date of the feasibility study by June 30, 2015. Although this response addresses part our recommendation, it does not outline any corrective actions for the repair of the inoperable CCTV cameras and surveillance system. We look forward to reviewing ICE's progress in the future. This recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

USSS Fully Complied with DHS Sensitive Systems Policies

USSS fully complied with DHS operational, technical, and management operational policies for its telecommunication room at JFK. We audited IT security controls of the USSS telecommunication room located at the JFK on-site building number 75. This location had a DHS OneNet connection and a network switch device. The telecommunications room was clean and well maintained. Visitor's logs were also maintained. Humidity and temperature sensor readings were within DHS policy guidelines. Since, the JFK location did not have an on-site server, vulnerability scans were not applicable.

Department's Nonconcurrence

Based on the Department's nonconcurrence with recommendation #6, we have added two additional recommendations that were not part of our draft report. Specifically, we recommend that the DHS CIO:

Recommendation #15:

Coordinate steps with DHS components located at JFK, to ensure their compliance with DHS Sensitive Systems Policy Directive 4300A, Section 1.4.8, and to designate the JFK CCTV cameras and surveillance systems as DHS IT systems.

We also recommend that the DHS Chief Privacy Officer:

Recommendation #16:

Require DHS components located at JFK to prepare PTAs and, as applicable, PIAs for the JFK CCTV cameras and surveillance systems as directed by privacy laws and policy.

Appendix A
Objectives, Scope, and Methodology

The DHS Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

This audit is part of a program to evaluate, on an ongoing basis, the implementation of DHS technical and information security policies and procedures at DHS sites. The objective of this program is to determine the extent to which critical DHS sites comply with the Department's technical and information security policies and procedures, according to *DHS Sensitive Systems Policy Directive 4300A* and its companion document, the *DHS 4300A Sensitive Systems Handbook*. Our primary focus was on evaluating the security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS IT infrastructure at this site. For example, we recorded humidity and temperature at different locations in the server rooms, and then averaged these readings. We also recorded humidity and temperature readings obtained from component sensors that existed in the rooms during fieldwork. We then compared these readings with DHS guidance.

We coordinated the implementation of this technical security evaluation program with the DHS Chief Information Security Officer. We interviewed TSA, CBP, ICE, and USSS, and other staff. We conducted site visits of TSA, CBP, ICE, and USSS facilities at and near JFK. We compared the DHS IT infrastructure that we observed onsite with the documented standards provided by the auditees.

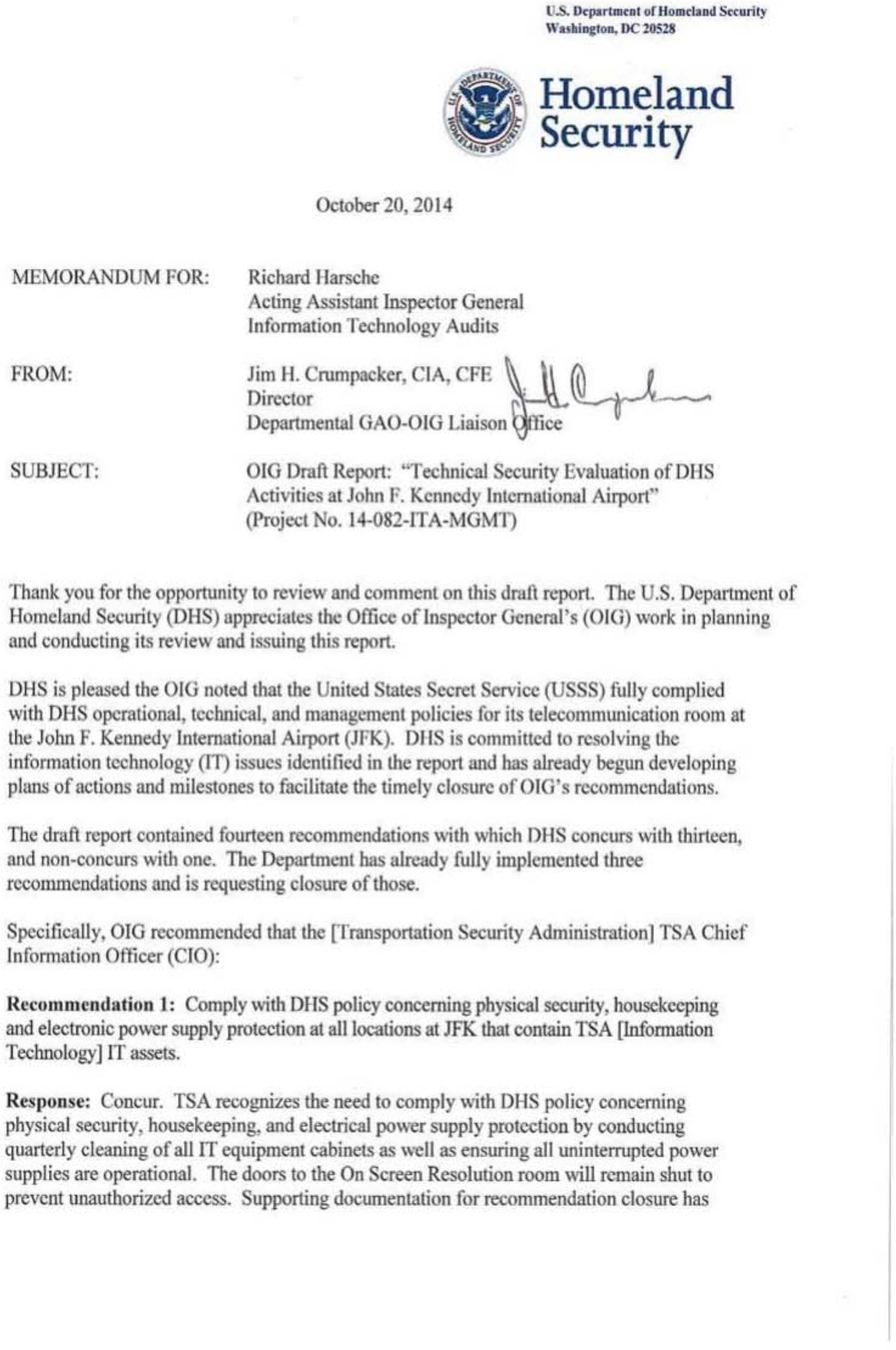
We reviewed the Information Assurance Compliance System documentation, such as the authority-to-operate letter, contingency plans, and system security plans. Additionally, we reviewed guidance provided by DHS to its components in the areas of system documentation, patch management, and wireless security. We also reviewed applicable DHS and components' policies and procedures, as well as Government-wide guidance. We gave briefings and presentations to DHS staff concerning the results of fieldwork and the information summarized in this report.

We conducted this performance audit between November 2013 and April 2014 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable

basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

We appreciate the efforts of DHS management and staff to provide the information and access necessary to accomplish this audit. The principal OIG points of contact for the audit are Richard Harsche, Acting Assistant Inspector General for Information Technology Audits, (202) 254-4100, and Sharon Huiswoud, Director, Information Systems Division, (202) 254-5451. Appendix D contains a major OIG contributors listing.

Appendix B
Management Comments to the Draft Report



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 20, 2014

MEMORANDUM FOR: Richard Harsche
Acting Assistant Inspector General
Information Technology Audits

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

SUBJECT: OIG Draft Report: "Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport"
(Project No. 14-082-ITA-MGMT)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG) work in planning and conducting its review and issuing this report.

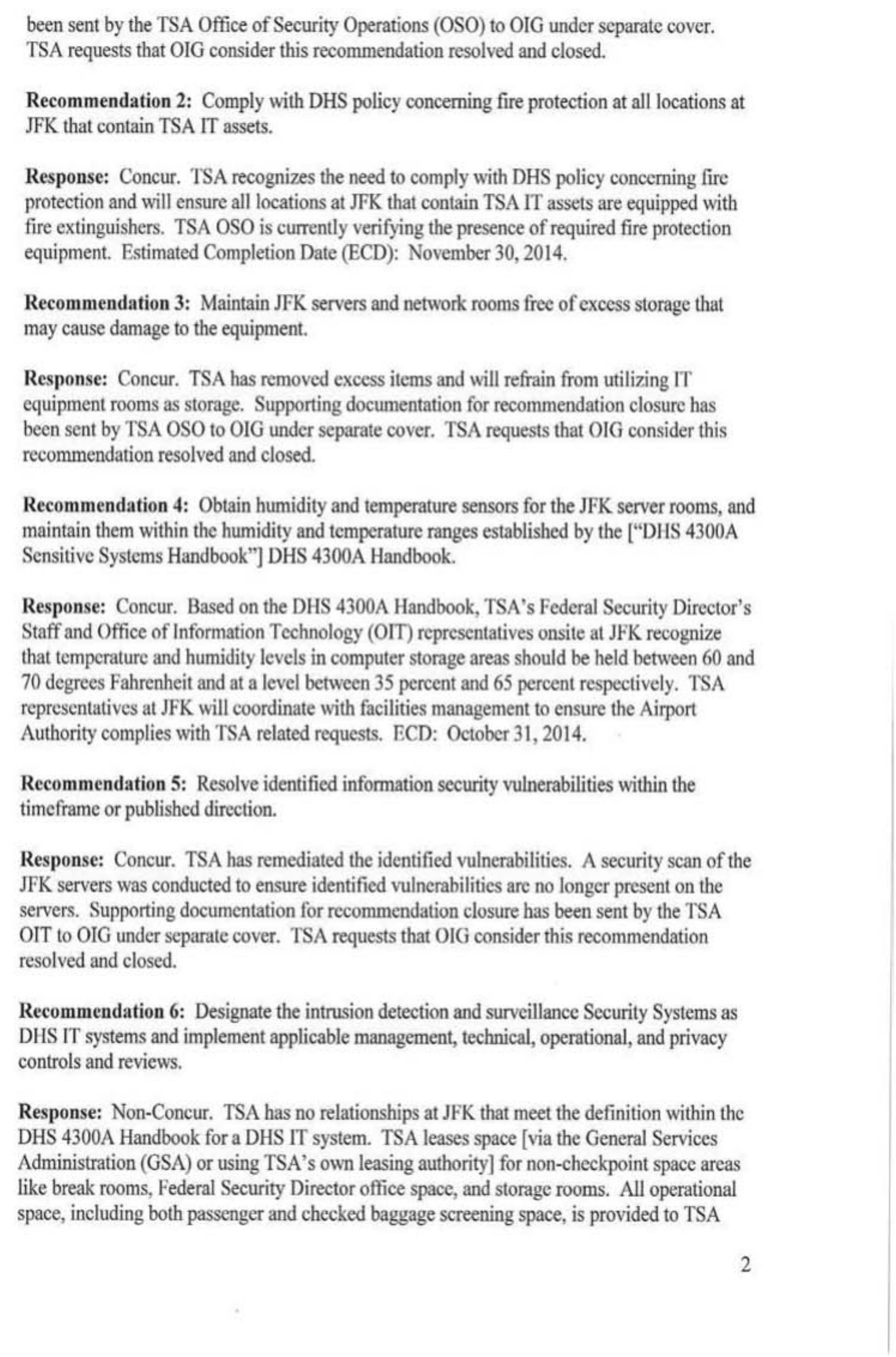
DHS is pleased the OIG noted that the United States Secret Service (USSS) fully complied with DHS operational, technical, and management policies for its telecommunication room at the John F. Kennedy International Airport (JFK). DHS is committed to resolving the information technology (IT) issues identified in the report and has already begun developing plans of actions and milestones to facilitate the timely closure of OIG's recommendations.

The draft report contained fourteen recommendations with which DHS concurs with thirteen, and non-concurs with one. The Department has already fully implemented three recommendations and is requesting closure of those.

Specifically, OIG recommended that the [Transportation Security Administration] TSA Chief Information Officer (CIO):

Recommendation 1: Comply with DHS policy concerning physical security, housekeeping and electronic power supply protection at all locations at JFK that contain TSA [Information Technology] IT assets.

Response: Concur. TSA recognizes the need to comply with DHS policy concerning physical security, housekeeping, and electrical power supply protection by conducting quarterly cleaning of all IT equipment cabinets as well as ensuring all uninterrupted power supplies are operational. The doors to the On Screen Resolution room will remain shut to prevent unauthorized access. Supporting documentation for recommendation closure has



been sent by the TSA Office of Security Operations (OSO) to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 2: Comply with DHS policy concerning fire protection at all locations at JFK that contain TSA IT assets.

Response: Concur. TSA recognizes the need to comply with DHS policy concerning fire protection and will ensure all locations at JFK that contain TSA IT assets are equipped with fire extinguishers. TSA OSO is currently verifying the presence of required fire protection equipment. Estimated Completion Date (ECD): November 30, 2014.

Recommendation 3: Maintain JFK servers and network rooms free of excess storage that may cause damage to the equipment.

Response: Concur. TSA has removed excess items and will refrain from utilizing IT equipment rooms as storage. Supporting documentation for recommendation closure has been sent by TSA OSO to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 4: Obtain humidity and temperature sensors for the JFK server rooms, and maintain them within the humidity and temperature ranges established by the ["DHS 4300A Sensitive Systems Handbook"] DHS 4300A Handbook.

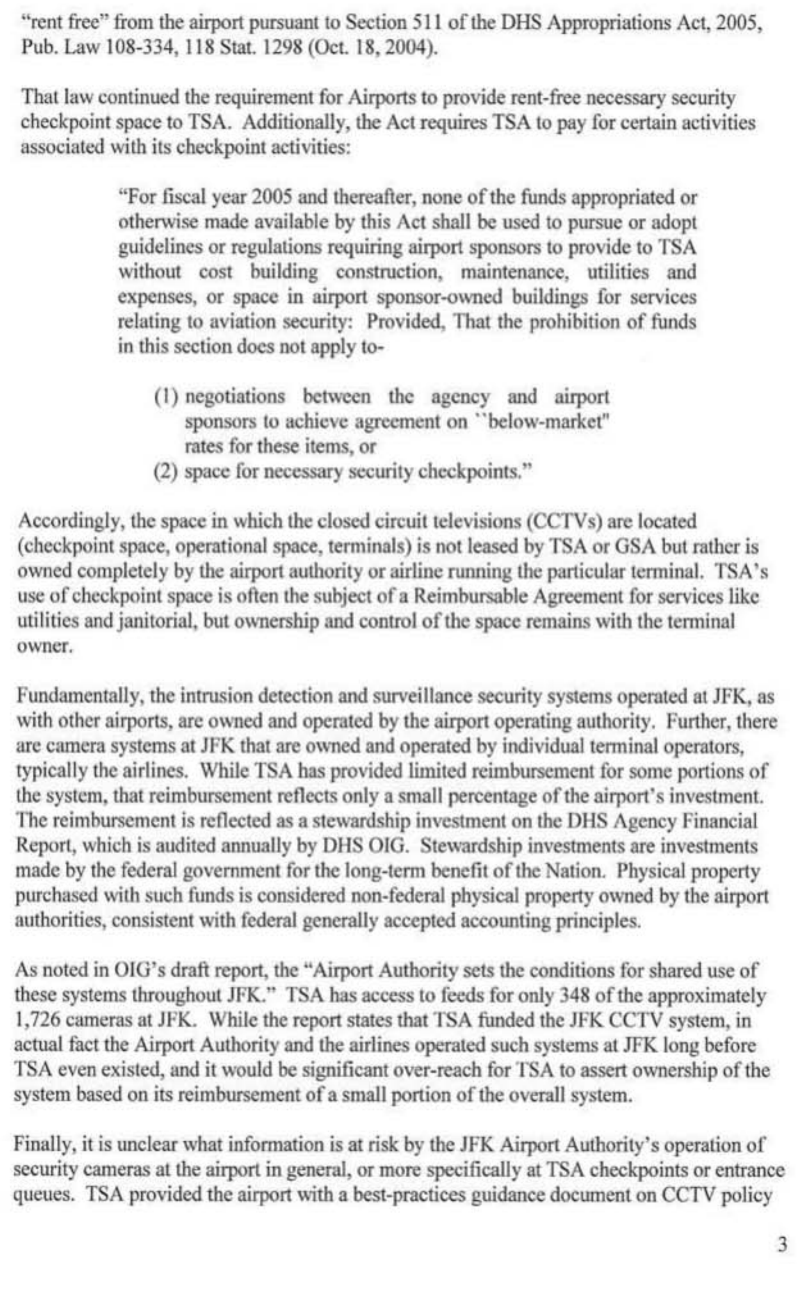
Response: Concur. Based on the DHS 4300A Handbook, TSA's Federal Security Director's Staff and Office of Information Technology (OIT) representatives onsite at JFK recognize that temperature and humidity levels in computer storage areas should be held between 60 and 70 degrees Fahrenheit and at a level between 35 percent and 65 percent respectively. TSA representatives at JFK will coordinate with facilities management to ensure the Airport Authority complies with TSA related requests. ECD: October 31, 2014.

Recommendation 5: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. TSA has remediated the identified vulnerabilities. A security scan of the JFK servers was conducted to ensure identified vulnerabilities are no longer present on the servers. Supporting documentation for recommendation closure has been sent by the TSA OIT to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 6: Designate the intrusion detection and surveillance Security Systems as DHS IT systems and implement applicable management, technical, operational, and privacy controls and reviews.

Response: Non-Concur. TSA has no relationships at JFK that meet the definition within the DHS 4300A Handbook for a DHS IT system. TSA leases space [via the General Services Administration (GSA) or using TSA's own leasing authority] for non-checkpoint space areas like break rooms, Federal Security Director office space, and storage rooms. All operational space, including both passenger and checked baggage screening space, is provided to TSA



"rent free" from the airport pursuant to Section 511 of the DHS Appropriations Act, 2005, Pub. Law 108-334, 118 Stat. 1298 (Oct. 18, 2004).

That law continued the requirement for Airports to provide rent-free necessary security checkpoint space to TSA. Additionally, the Act requires TSA to pay for certain activities associated with its checkpoint activities:

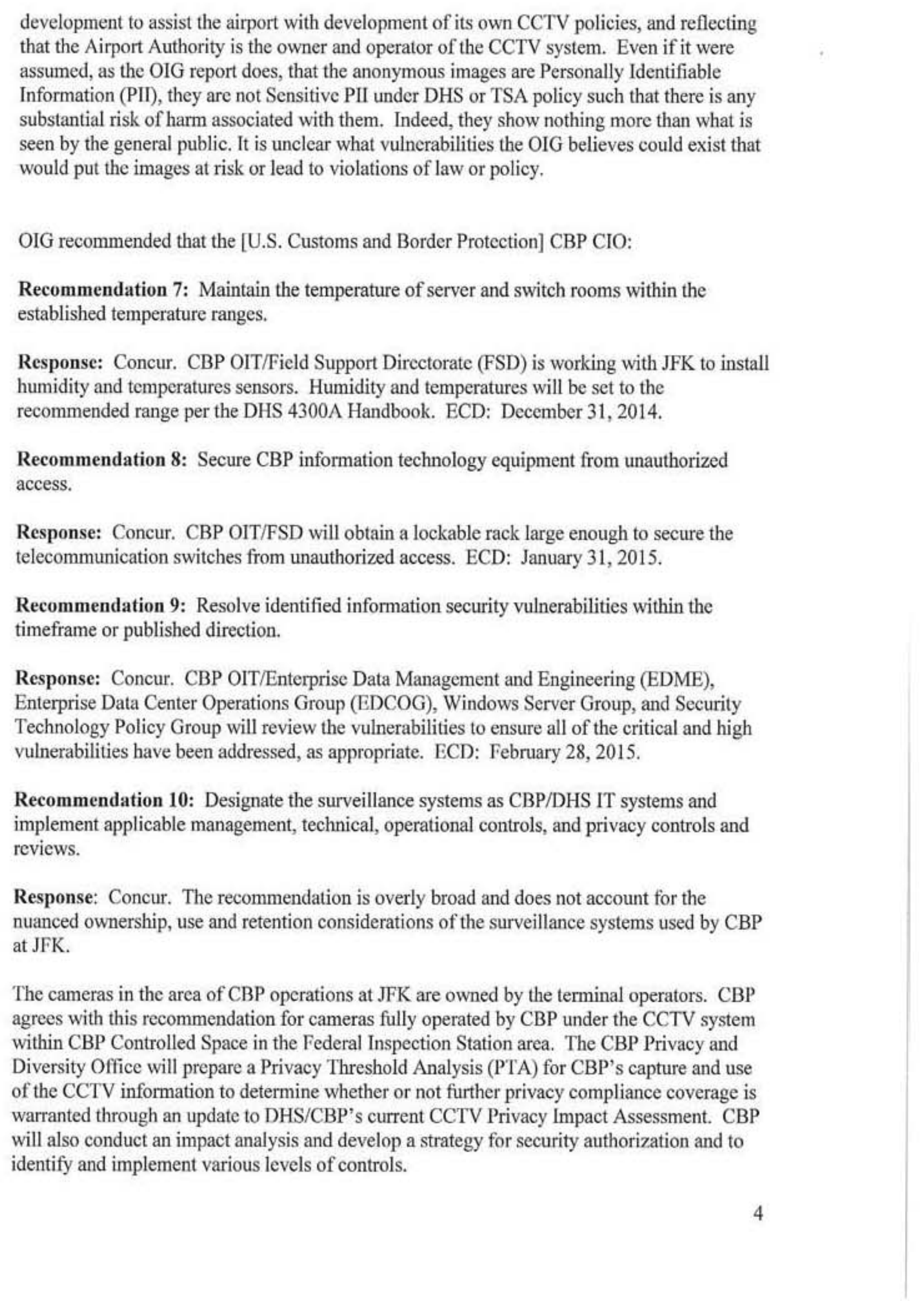
> "For fiscal year 2005 and thereafter, none of the funds appropriated or otherwise made available by this Act shall be used to pursue or adopt guidelines or regulations requiring airport sponsors to provide to TSA without cost building construction, maintenance, utilities and expenses, or space in airport sponsor-owned buildings for services relating to aviation security: Provided, That the prohibition of funds in this section does not apply to-
>
> (1) negotiations between the agency and airport sponsors to achieve agreement on ``below-market" rates for these items, or
> (2) space for necessary security checkpoints."

Accordingly, the space in which the closed circuit televisions (CCTVs) are located (checkpoint space, operational space, terminals) is not leased by TSA or GSA but rather is owned completely by the airport authority or airline running the particular terminal. TSA's use of checkpoint space is often the subject of a Reimbursable Agreement for services like utilities and janitorial, but ownership and control of the space remains with the terminal owner.

Fundamentally, the intrusion detection and surveillance security systems operated at JFK, as with other airports, are owned and operated by the airport operating authority. Further, there are camera systems at JFK that are owned and operated by individual terminal operators, typically the airlines. While TSA has provided limited reimbursement for some portions of the system, that reimbursement reflects only a small percentage of the airport's investment. The reimbursement is reflected as a stewardship investment on the DHS Agency Financial Report, which is audited annually by DHS OIG. Stewardship investments are investments made by the federal government for the long-term benefit of the Nation. Physical property purchased with such funds is considered non-federal physical property owned by the airport authorities, consistent with federal generally accepted accounting principles.

As noted in OIG's draft report, the "Airport Authority sets the conditions for shared use of these systems throughout JFK." TSA has access to feeds for only 348 of the approximately 1,726 cameras at JFK. While the report states that TSA funded the JFK CCTV system, in actual fact the Airport Authority and the airlines operated such systems at JFK long before TSA even existed, and it would be significant over-reach for TSA to assert ownership of the system based on its reimbursement of a small portion of the overall system.

Finally, it is unclear what information is at risk by the JFK Airport Authority's operation of security cameras at the airport in general, or more specifically at TSA checkpoints or entrance queues. TSA provided the airport with a best-practices guidance document on CCTV policy



development to assist the airport with development of its own CCTV policies, and reflecting that the Airport Authority is the owner and operator of the CCTV system. Even if it were assumed, as the OIG report does, that the anonymous images are Personally Identifiable Information (PII), they are not Sensitive PII under DHS or TSA policy such that there is any substantial risk of harm associated with them. Indeed, they show nothing more than what is seen by the general public. It is unclear what vulnerabilities the OIG believes could exist that would put the images at risk or lead to violations of law or policy.

OIG recommended that the [U.S. Customs and Border Protection] CBP CIO:

Recommendation 7: Maintain the temperature of server and switch rooms within the established temperature ranges.

Response: Concur. CBP OIT/Field Support Directorate (FSD) is working with JFK to install humidity and temperatures sensors. Humidity and temperatures will be set to the recommended range per the DHS 4300A Handbook. ECD: December 31, 2014.

Recommendation 8: Secure CBP information technology equipment from unauthorized access.

Response: Concur. CBP OIT/FSD will obtain a lockable rack large enough to secure the telecommunication switches from unauthorized access. ECD: January 31, 2015.

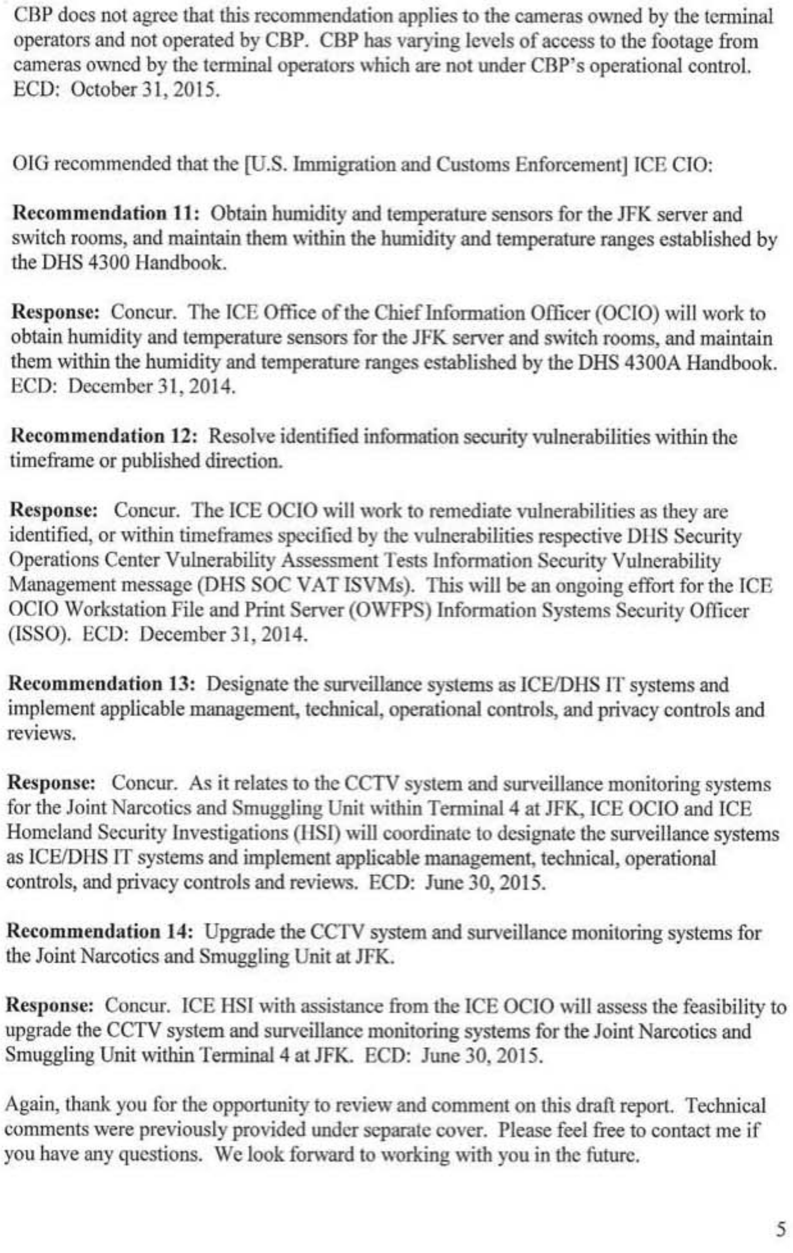
Recommendation 9: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. CBP OIT/Enterprise Data Management and Engineering (EDME), Enterprise Data Center Operations Group (EDCOG), Windows Server Group, and Security Technology Policy Group will review the vulnerabilities to ensure all of the critical and high vulnerabilities have been addressed, as appropriate. ECD: February 28, 2015.

Recommendation 10: Designate the surveillance systems as CBP/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Response: Concur. The recommendation is overly broad and does not account for the nuanced ownership, use and retention considerations of the surveillance systems used by CBP at JFK.

The cameras in the area of CBP operations at JFK are owned by the terminal operators. CBP agrees with this recommendation for cameras fully operated by CBP under the CCTV system within CBP Controlled Space in the Federal Inspection Station area. The CBP Privacy and Diversity Office will prepare a Privacy Threshold Analysis (PTA) for CBP's capture and use of the CCTV information to determine whether or not further privacy compliance coverage is warranted through an update to DHS/CBP's current CCTV Privacy Impact Assessment. CBP will also conduct an impact analysis and develop a strategy for security authorization and to identify and implement various levels of controls.



CBP does not agree that this recommendation applies to the cameras owned by the terminal operators and not operated by CBP. CBP has varying levels of access to the footage from cameras owned by the terminal operators which are not under CBP's operational control. ECD: October 31, 2015.

OIG recommended that the [U.S. Immigration and Customs Enforcement] ICE CIO:

Recommendation 11: Obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Response: Concur. The ICE Office of the Chief Information Officer (OCIO) will work to obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300A Handbook. ECD: December 31, 2014.

Recommendation 12: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. The ICE OCIO will work to remediate vulnerabilities as they are identified, or within timeframes specified by the vulnerabilities respective DHS Security Operations Center Vulnerability Assessment Tests Information Security Vulnerability Management message (DHS SOC VAT ISVMs). This will be an ongoing effort for the ICE OCIO Workstation File and Print Server (OWFPS) Information Systems Security Officer (ISSO). ECD: December 31, 2014.

Recommendation 13: Designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Response: Concur. As it relates to the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK, ICE OCIO and ICE Homeland Security Investigations (HSI) will coordinate to designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews. ECD: June 30, 2015.

Recommendation 14: Upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit at JFK.

Response: Concur. ICE HSI with assistance from the ICE OCIO will assess the feasibility to upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ECD: June 30, 2015.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Appendix C
DHS Activities at JFK Airport

Transportation Security Administration

TSA uses technology to screen passengers and baggage on all departing flights at each of the JFK terminals and to support operation management at nearby office buildings.

We audited IT security controls at the following TSA locations:

- JFK Terminals 1, 2, 4, 5, 7, and 8,
- Office of the Federal Security Director, Jamaica, NY, and
- Office of Federal Air Marshal Service (FAMS), Jamaica, NY.

TSA staff at these locations use the following systems:

- Federal Air Marshal Service Network (FAMSNet) – provides the IT infrastructure to support the FAMS law enforcement mission to help detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews. FAMSNet provides Internet access as well as internal access to FAMS information systems including, but not limited to, email, databases, file sharing, printing, and a number of critical administrative and enforcement related programs. FAMSNet also provides a communication pathway to third-party and Government networks, such as those used by other DHS components, the Federal Aviation Administration, and other State and local law enforcement entities.
- Infrastructure Core System – provides electronic file and print capabilities to the entire TSA user community.
- TSA End User Computing System – provides TSA employees and contractors with desktops, laptops, local printers, mobile devices and other end user computing applications.
- Security Technology Integrated Program – combines many different types of components, including transportation security equipment, servers and storage, software/application products, and databases. Users physically access the transportation security equipment to perform screening or other administrative

functions. TSA's Office of Security Capabilities is the owner of the Security Technology Integrated Program.

- Transportation Security Administration Network (TSANet) – provides connectivity in airports for TSA users. TSANet consists of a geographically-dispersed wide area network and each site's local area network. The networks are connected to the DHS One Network (OneNet) and have been designated a mission essential system.

U.S. Customs and Border Protection

CBP employs over 1,600 staff at JFK to protect the United States from drug and human smugglers, agricultural diseases and pests, and terrorists. CBP personnel also:

- review flight data for terrorist-related activities,
- collect duties, and
- assess fines and civil penalties.

Also, CBP staff at nearby locations use IT assets to perform cargo and outbound passenger review and targeting. In addition, JFK CBP employees operate and maintain the international mail facility.

We audited IT security controls at the following CBP locations:

- JFK Terminals 1, 4, 5, 7, and 8, and
- CBP buildings Number 77 and 250, located in Jamaica, NY.

CBP staff at these locations use the following systems:

- Northeast Field Local Area Network – provides the general support network infrastructure for DHS/CBP users and electronic communications tools, which enables the execution of official duties. The Northeast Field Local Area Network includes 290 geographically dispersed sites using 9,000 devices connected to the OneNet to provide application services to CBP field offices.

- CBP Network Operations Center – maintains the performance, management, and administration of the core network and underlying supporting environment at CBP field site locations. In addition, the center deploys and maintains a network management system and a suite of network devices that collect and report real-time network security information. Further, the center manages the flow of information within interconnected systems in accordance with DHS Sensitive Security Policy.

- Windows 7 PC Client 6.1 – used as the Windows 7 standard desktop image for CBP workstations. Windows 7 PC Client 6.1 consists of a set of standard configurations and installs application software and configures systems according to DHS and CBP technical standards.

- The Windows File and Print System – provides CBP with file and printing services using the Microsoft Windows Server 2008 x 64 platforms.

- Treasury Enforcement Communication System (TECS) – supports enforcement and inspection operations for several components of DHS and is a vital tool for local, State, tribal, and Federal Government law enforcement and intelligence communities.6 TECS includes several subsystems for enforcement, inspection, and intelligence records relevant to the antiterrorist and law enforcement mission of CBP and other Federal agencies.

[6] Formerly known as the Treasury Enforcement Communications System, TECS is no longer an acronym (effective December 19, 2008) and is principally owned and managed by CBP.

U.S. Immigration and Customs Enforcement

The New York ICE Office of the Special Agent in Charge is responsible for the administration and management of all investigative and enforcement activities within its geographical boundaries. Within the New York Special Agent in Charge office, the Homeland Security Investigations Airport Group is responsible for the identification, disruption, and dismantlement of transnational criminal organizations attempting to exploit vulnerabilities within the air transportation system at JFK. The Homeland Security Investigations Airport Group's areas of concern at JFK include:Contraband smuggling,

- Currency smuggling,
- National security,
- Human smuggling/trafficking,
- Sexual tourism,
- Insider threat, and
- Theft and trafficking of cultural heritage and art.

The JFK Office of Professional Responsibility investigates criminal and administrative misconduct committed by ICE and CBP employees and contractors. This office also addresses complaints of people pretending to be ICE and CBP employees or attempted bribery.

We audited IT security controls at the following ICE locations:

- The Special Agent in Charge New York Office, located in Building No. 75,
- Office of Professional Responsibility, located in Building No. 75, and
- Joint Narcotics and Smuggling Unit, located in JFK Terminal 4.

ICE staff at these locations use the following systems:

- Office File and Print Servers – provide workstation, laptop, print services, and file capability to all ICE employees. File servers provide a networked file repository and print servers allow networked printing.

- ICE Communication over Networks – provides support for all network devices and data communications used by ICE and at 287(g) sites.[7]
- A communication surveillance and analysis system that helps Homeland Security Investigations staff to gather intelligence and collect live data in support of ICE's law enforcement mission. Specifically, the system assembles historical telephone records, monitors telephone and Internet communications, and permits searches of warrant data from online providers. The communication surveillance and analysis system connects to the ICE network infrastructure or on a separate standalone network. This is not a designated mission essential system.

U.S. Secret Service

USSS have nine agents and two administrative personnel located at JFK that report directly to the USSS New York Field Office in Brooklyn, NY. This office is the only USSS office located at an airport.

The agents assigned to the office handle between 750 and 800 arrivals and departures of USSS protected individuals/groups, including Prime Ministers and current and former U.S. Presidents and immediate family members, at JFK and LaGuardia Airports. Each September, the United Nations General Assembly in New York City impacts the JFK Resident Office with over 300 arrivals and departures at JFK and LaGuardia Airports and an additional 42 temporarily assigned agents/officers.

The office also works closely with CBP to seize counterfeit United States currency entering JFK Airport at the passenger and cargo terminals. Since May 2010, DHS seized United States currency totaling over $4 million. The employees of the USSS office use Windows 7, Office 2010, and web—based applications. The service's New York Field Office Technical Operations Squad performs all IT updates, equipment repairs, and installation of new equipment.

[7] The 287(g) program, under the *Immigration and Nationality Act*, as amended, allows a state and local law enforcement entity to receive delegated authority for immigration enforcement within its jurisdiction.

Appendix D
Major Contributors to This Report

Sharon Huiswoud, IT Audit Director
Sharell Grady, IT Audit Manager
Beverly Dale, IT Senior Auditor
Robert Durst, Senior Program Analyst
Frederick Shappee, Senior Program Analyst
Daniel McGrath, Referencer

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
DHS CISO
DHS CISO Audit Liaison
CBP CIO
CBP Audit Liaison
ICE CIO
ICE Audit Liaison
TSA CIO
TSA Audit Liaison
USSS CIO
USSS Audit Liaison
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

Requester’s Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

4 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

OFFICE OF INSPECTOR GENERAL

Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport (Redacted) (Revised)

Homeland Security

January 16, 2015

OIG-15-18 (Revised)

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

January 16, 2015

MEMORANDUM FOR: The Honorable Chip Fulghum
Acting Under Secretary for Management

FROM: John Roth John Roth
Inspector General

SUBJECT: *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport*

Attached for your information is our revised final report, *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport.* This report contains findings and recommendations for improving security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS information technology infrastructure at this airport.

The procedural history of this report elicits an unfortunate commentary on the manner in which the Department handled this matter and bears review:

- We provided a draft of this report on July 22, 2014 to the Chief Information Officer for review. Pursuant to *Department of Homeland Security Directive 077-01, Follow-up, and Resolution for Office of Inspector General Report Recommendations,* we asked for agency comments, including a sensitivity review, within 30 days of receipt of the draft. This would have made the report due on or about August 22, 2014. Almost a week later, on August 27, 2014, the DHS Chief of Staff requested an extension to provide a response and technical comments. I granted the extension until September 17, 2014.

- On October 20, 2014, nearly 60 days after the original due date for agency comments, the Departmental GAO-OIG Liaison Office finally conveyed to us TSA's response to our request for a sensitivity review by marking several passages in the report as SSI. I disagree with this determination.

- On November 19, 2014, I sent a formal challenge memo to TSA Administrator John Pistole expressing my disagreement. Administrator Pistole had authority over all TSA programs and operations, including oversight of the SSI programs, and is my counterpart in DHS' leadership.

- Having received no reply, on December 16, 2014, I wrote to Administrator Pistole a second time, noting that this report had languished as a result of TSA's sensitivity review, and again requesting that he remove the SSI deletions from the report. As with the November 19, 2014 letter, I received no reply.

- Finally, on January 13, 2015, over five months after submitting the report for sensitivity review, and two months after writing to Administrator Pistole, I received a decision, not from the Acting TSA Administrator, but from the head of the SSI program office – the very same office that initially and improperly marked the information as SSI. Not surprisingly, the office affirmed its original redaction to the report.

I am disappointed in both the substance of the decision as well as its lack of timeliness. In 2006, Congress, concerned about delays in appeals of this nature, directed the Department to revise DHS Management Directive 11056.1 to require TSA to require timely SSI reviews. Given the clear requirement for timely SSI reviews in response to requests from the *public*, we hoped that TSA would approach an SSI appeal from the *Inspector General* with similar diligence, especially because TSA was aware of our deadlines.

Now, to meet our reporting requirement, we are compelled to publish a redacted report with SSI markings and will again ask the head of TSA to overrule the SSI program office's decision.

I believe that this report should be released in its entirety in the public domain. I challenged TSA's determination because this type of information has been disclosed in other reports without objection from TSA, and because the language marked SSI reveals generic, non-specific vulnerabilities that are common to virtually all systems and would not be detrimental to transportation security. My auditors, who are experts in computer security, have assured me that the redacted information would not compromise transportation security. Our ability to issue reports that are transparent, without unduly restricting information, is key to accomplishing our mission. Congress, when it passed the *Reducing Over-Classification Act* in 2010, found that over-classification "interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information."

Consistent with our responsibilities under the *Inspector General Act*, and in compliance with 49 CFR 1520, we will provide appropriately marked and unredacted copies of our report to appropriate Congressional committees with oversight and appropriation responsibility for the Department of Homeland Security. We will post a redacted version of the report on our website pending a decision from the Acting TSA Administrator.

I appreciate your attention to this matter. Should you have any questions, please call me, or your staff may contact Sondra McCauley, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4041.

Attachments

cc: Melvin Carraway, Acting Administrator
Transportation Security Administration

The Honorable R. Gil Kerlikowske
Commissioner, U.S. Customs and Border Protection

The Honorable Sarah Saldaña
Assistant Secretary, U.S. Immigration and Customs Enforcement

Joseph Clancy, Acting Director
United States Secret Service

HIGHLIGHTS

Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport

January 16, 2015

Why We Did This

We evaluated technical and information security policies and procedures of Department of Homeland Security components at the John F. Kennedy International Airport. Our evaluation focused on how these components have implemented operational, technical, and management controls for computer security at the airport and nearby locations.

What We Recommend

We made recommendations addressing the control deficiencies identified in this report. The information technology security controls implemented at several sites had deficiencies that, if exploited, could have resulted in the loss of confidentiality, integrity, and availability of the components' information technology systems.

What We Found

The Department's information technology security controls implemented at several sites had deficiencies that, if exploited, could have resulted in the loss of confidentiality, integrity, and availability of the components' information technology systems. We identified numerous deficiencies in the information technology security controls associated with the Transportation Security Administration. Additionally, operational environmental controls and security documentation needed improvement. Further, information security vulnerabilities were not resolved timely. Technical security controls for Customs and Border Protection and Immigration and Customs Enforcement information technology resources also needed improvement. The Transportation Security Administration, Customs and Border Protection, and Immigration and Customs Enforcement did not perform required security authorization or privacy reviews on closed–circuit television and surveillance monitoring room technology. The U.S. Secret Service fully complied with DHS sensitive security policies at the airport.

Management Response

We briefed the DHS Chief Information Security Officer and the components on the results of our audit. The draft report included 14 recommendations and DHS concurred with 13 of the 14 recommendations. DHS did not concur with recommendation number six. We do not agree with DHS's response to this recommendation. The response does not provide for corrective actions to address the security and privacy concerns identified in our report. Therefore, we issued two additional recommendations, one for the DHS Chief Information Officer and another for the DHS Chief Privacy Officer.

Errata page for OIG-15-18

Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport (Redacted)

Changes made for Redactions page 5, 1st paragraph and figure 2 (see below):

Revised SSI marking redactions applied.

Change made to the Management Comments and OIG Analysis section, page 31, 1st paragraph (see below):

The following statement has been removed from our report for clarity:

We consider these recommendations resolved, but open pending verification of corrective and planned actions and supportive documentation.

Change made to the Management Comments and OIG Analysis section, page 39, 1st paragraph (see below):

The following statement has been removed from our report for clarity:

We consider these recommendations resolved, but open pending verification of corrective and planned actions and supportive documentation.

The revisions did not change the findings or recommendations made in this report.

Table of Contents

Executive Summary ... 1

Background ... 2

Results of Audit ... 4

TSA Did Not Comply Fully with DHS Sensitive Systems Policies ... 4
Recommendations ... 16
Management Comments and OIG Analysis ... 17

CBP Did Not Comply Fully with DHS Sensitive Systems Policies ... 20
Recommendations ... 26
Management Comments and OIG Analysis ... 27

ICE Did Not Comply Fully with DHS Sensitive Systems Policies ... 29
Recommendations ... 33
Management Comments and OIG Analysis ... 34

USSS Fully Complied with DHS Sensitive Systems Policies ... 36

Department's Noncurrence ... 36

Appendixes

Appendix A: Objectives, Scope, and Methodology ... 37
Appendix B: Management Comments to the Draft Report ... 39
Appendix C: DHS Activities at JFK Airport ... 44
Appendix D: Major Contributors to This Report ... 49
Appendix E: Report Distribution ... 50

Abbreviations

Airport Authority	Port Authority of New York and New Jersey
CBP	U.S. Customs and Border Protection
CCTV	closed-circuit television
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security

FAMS	Federal Air Marshall Service
FAMSNet	Federal Air Marshall Service Network
GAO	Government Accountablity Office
ICE	U.S. Immigration and Customs Enforcement
IT	information technology
JFK	John F. Kennedy International Airport
OIG	Office of Inspector General
OMB	Office of Management and Budget
OneNet	DHS One Network
PIA	privacy impact assessment
PII	personally identifiable information
PTA	privacy threshold assessment
Security System	Airport Authority Selected Surveillance Systems
TECS	Treasury Enforcement Communication System
TSA	Transportation Security Administration
TSANet	Transportation Security Administration Network
UPS	uninterruptible power supply
USSS	United States Secret Service

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Executive Summary

As part of our Technical Security Evaluation Program, we evaluated technical and information security policies and procedures of Department of Homeland Security components at the John F. Kennedy International Airport. Four Department components – the Transportation Security Administration, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Secret Service – operate information technology systems that support homeland security operations at this major airport.

Our evaluation focused on how these components have implemented operational, technical, and management controls for computer security at the airport and nearby locations. We performed onsite inspections of the areas where these assets were located, interviewed departmental staff, and conducted technical tests of computer security controls. We also reviewed applicable policies, procedures, and other relevant documentation.

The Department's sensitive system security policies, the information technology security controls implemented at several sites had deficiencies that, if exploited, could have resulted in the loss of confidentiality, integrity, and availability of the components' information technology systems. We identified numerous deficiencies in the information technology security controls associated with the Transportation Security Administration. Additionally, operational environmental controls and security documentation needed improvement. Further, information security vulnerabilities were not resolved timely. Technical security controls for Customs and Border Protection and Immigration and Customs Enforcement information technology resources also needed improvement. The Transportation Security Administration, Customs and Border Protection, and Immigration and Customs Enforcement did not perform required security authorization or privacy reviews on closed–circuit television and surveillance monitoring room technology. The U.S. Secret Service fully complied with DHS sensitive security policies at the airport.

The draft report included 14 recommendations and DHS concurred with 13 of the 14 recommendations. DHS did not concur with recommendation number six. We do not agree with DHS's response to this recommendation, as it does not provide for corrective actions to address the security and privacy concerns identified in our report. To help ensure that these security and privacy concerns get addressed properly, we issued two additional recommendations for the DHS Chief Information Officer and DHS Chief Privacy Officer. We have included a copy of the Department's comments to the draft report in their entirety in appendix B.

Background

We designed our Technical Security Evaluation Program to provide senior Department of Homeland Security officials with timely information on whether they had properly implemented DHS information technology (IT) security policies at critical sites. Our program audit was based on the requirements identified within *DHS Sensitive Systems Policy Directive 4300A,* version 10.0, which provides direction to DHS component managers and senior executives regarding the management and protection of sensitive systems. This directive and an associated handbook outline policies on the operational, technical, and management controls necessary to ensure confidentiality, integrity, and availability within the DHS IT infrastructure and operations. These controls are as follows:

- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people to improve system security. For example, operational control mechanisms include physical access controls that restrict the entry and exit of personnel from an area, such as an office building, data center, or room, where sensitive information is accessed, stored, or processed.

- **Technical Controls** – Focus on security controls executed by information systems. These controls provide automated protection from unauthorized access; facilitate detection of security violations; and support applications and data security requirements. For example, technical controls include passwords for systems.

- **Management Controls** – Focus on managing both the system information security controls and system risk. These controls include risk assessments, rules of behavior, and ensuring that security is an integral part of both system development and IT procurement processes.

We evaluated security controls for IT systems that support homeland security operations of the Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Secret Service (USSS) at John F. Kennedy International Airport (JFK). Figure 1 shows Terminal Four at JFK.

Figure 1-JFK Terminal Four

JFK is the sixth busiest airport in the United States. With arrivals and departures from almost every international airline in the world, JFK is an international gateway for passengers and heavy freight. Below are some facts about JFK.

- JFK, on the Jamaica Bay in New York City, is a designated port of entry.[1] The airport covers over 4,930 acres, including 30 miles of roadway. JFK has 6 operating airline terminals and more than 125 airline gates.

- Port Authority of New York and New Jersey (Airport Authority) operates JFK under a lease with the City of New York since 1947, with the current lease continuing until 2050. The Airport Authority has invested over $10 billion in the airport.

- JFK contributes about $30.6 billion in economic activity annually to the New York/New Jersey region, generating approximately $4.2 billion in direct wages; 71,000 jobs and indirect wages of $30.5 billion for 213,400 jobs.

- JFK is a leading international air cargo center. This facility has more than four million square feet of office and warehouse space dedicated to cargo operations serving the New York and New Jersey region. The entire air cargo area has automated and computer-controlled terminals containing one or more restricted access sites.

[1] Port of entry is defined as a designated controlled entry points into the United States from foreign countries.

See appendix C for specific details of DHS component activities at the JFK airport.

Results of Audit

TSA Did Not Comply Fully with DHS Sensitive Systems Policies

TSA did not comply fully with DHS operational, technical, and management policies for its servers and switches operating at JFK. Specifically, physical security and access controls for numerous TSA server rooms and communication closets were deficient. Additionally, TSA had not implemented known software patches to its servers at JFK. Finally, TSA did not designate the closed-circuit television (CCTV) cameras as a DHS IT system nor did it implement the applicable, operational, technical, and managerial controls for the cameras. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability, of the data stored, transmitted, and processed by TSA at JFK.

Operational Controls

We evaluated TSA server rooms and communication closets containing IT assets at JFK. We identified operational controls that did not conform fully to DHS policies. Specifically, we identified deficiencies in physical security, visitor logs, the fire protection system, storage and housekeeping, electronic power supply protection, and humidity and temperature controls.

Physical Security

Adequate access controls have not been established limiting access to TSA sensitive equipment in JFK terminals. For example, [redacted] located [redacted] contained DHS locked equipment cabinets located [redacted] with non-DHS IT equipment. According to TSA staff, technical representatives did not know the total number of non-DHS personnel that had access to [redacted] In addition, [redacted] contained unsecured TSA equipment and were accessible to non-DHS individuals. Specifically, as shown in figure 2, a TSA [redacted] cabinet was located [redacted] airport. The doors between the two areas did not lock, and airport employees walked through the area. [redacted]

[redacted]

[redacted]

The door to the secure Explosive Detection Systems room, where TSA reviews x-ray images of luggage to determine if suspicious checked luggage requires additional inspection, was propped open to vent a portable air conditioning unit, violating physical security controls. Figures 3a, 3b, and 3c show the required access control into the room, a secondary door to the room left open, and an air conditioning unit venting hot air out through the open door.

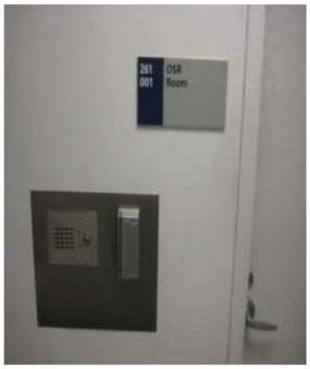


Figure 3a-Access Control

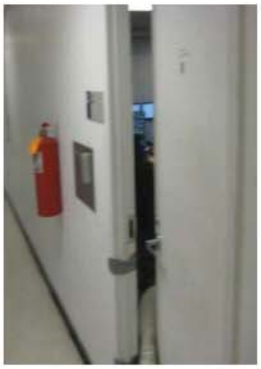


Figure 3b-Unsecured Door

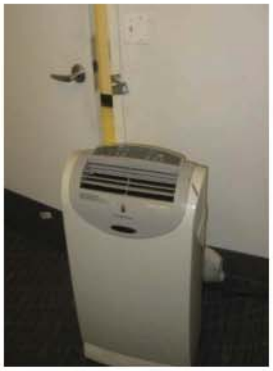


Figure 3c-Climate Control

According to DHS Sensitive System Policy Directive 4300A:

> Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.

Physical security vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of TSA data. Unauthorized access to TSA server rooms may result in the loss of IT processing capability used for passenger and baggage screening.

Visitor Logs

At JFK, TSA did not have visitor logs in any of its communication rooms to document the entry and exit of visitors to these rooms that contain sensitive IT equipment.

According to DHS Sensitive System Policy Directive 4300A:

> Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data. They shall be escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.

When unauthorized individuals gain access to locations where sensitive computing resources reside, there is an increased risk of system compromise and data confidentiality, integrity, and availability concerns.

Fire Protection System

Fire protection, detection, and suppression controls were not present in many TSA communication rooms. Specifically, 14 of the 21 rooms inspected that contained sensitive equipment did not have fire extinguishers. Additionally, 8 of the 21 rooms did not have a fire suppression system installed. As a result, 5 rooms were in violation of fire protection policy. Table 1 shows the existence or lack of fire protection equipment at the locations inspected.

Table 1-TSA Fire Protection

TSA Fire Protection			
Identification of the room	**Smoke Detector**	**Fire Extinguisher**	**Fire Suppression**
TSA Location 1	Yes	No	Yes
TSA Location 2	Yes	No	Yes
TSA Location 3, TSA/FAMS	No	No	Yes
TSA Location 4, Terminal 1	No	No	No
TSA Location 5, Terminal 1	No	No	Yes
TSA Location 6 Terminal 1	Yes	No	Yes
TSA Location 7, Terminal 2	No	No	Yes
TSA Location 8, Terminal 4	No	No	Yes
TSA Location 9, Terminal 4	Yes	Yes	No
TSA Location 10, Terminal 4	No	No	No
TSA Location 11, Terminal 4	Yes	Yes	No
TSA Location 12, Terminal 5	No	No	Yes
TSA Location 13, Terminal 5	Yes	No	Yes
TSA Location 14, Terminal 5	No	Yes	Yes
TSA Location 15, Terminal 7	No	No	No
TSA Location 16, Terminal 7	No	Yes	No
TSA Location 17, Terminal 7	No	No	No
TSA Location 18, Terminal 7	No	No	No
TSA Location 19, Terminal 8	Yes	Yes	Yes
TSA Location 20, Terminal 8	No	Yes	Yes
TSA Location 21, Terminal 8	No	Yes	Yes

According to DHS 4300A Sensitive Systems Handbook:

> Fire protection systems should be serviced by professionals on a recurring basis to ensure that the systems stay in proper working order. The following should be considered when developing a fire protection strategy:
>
> - When a centralized fire suppression system is not available, fire extinguishers should be readily available.
> - Facilities should make available/provide Class C fire extinguishers, designed for use with electrical fire and other types of fire.
> - Fire extinguishers should be located in such a way that a user would not need to travel more than 50 feet to retrieve one.

Compounding the issue of fire detection and mitigation, only 7 of 21 the rooms inspected contained smoke detectors. Smoke detectors alert the appropriate personnel of a potential fire and possible hazard.

The DHS 4300A Sensitive Systems Handbook also states:

> In addition to the physical security controls discussed above, facility managers and security administrators must also ensure that environmental controls are established, documented, and implemented to provide needed protection in the following areas:
>
> - Fire protection, detection, and suppression

In addition to DHS 4300A Sensitive Systems Handbook, TSA's Information Assurance Handbook states:

> The Facility Security manager shall employ and maintain fire suppression and detection devices/systems (to include sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors) for the TSA facility information systems that are supported by an independent energy source. When centralized fire suppression is not available, Class C fire extinguishers should be readily available. Each class C fire extinguisher

should be located in such a way that the user would not need to travel more than 50 feet to retrieve it.

The lack of fire notification capabilities and unmitigated suppression system vulnerabilities place at risk the availability of TSA data. For example, sensitive equipment damaged by fire may not be available for TSA's passenger and baggage screening processes.

Storage and Housekeeping

Several TSA communication closets located in the JFK terminals contained storage items and cleaning supplies. For example, we found TSA equipment on top of an unlocked TSA telecommunication cabinet surrounded by a ladder, boxes, trash, and cleaning supplies. The ladder, boxes, and cleaning supplies are all harmful to IT equipment. Additionally, there was no sign in sheet, and non-TSA personnel used the room for equipment storage. Figures 4 and 5, show cleaning supplies and maintenance equipment stored with TSA IT hardware in a communication room and communication closet.

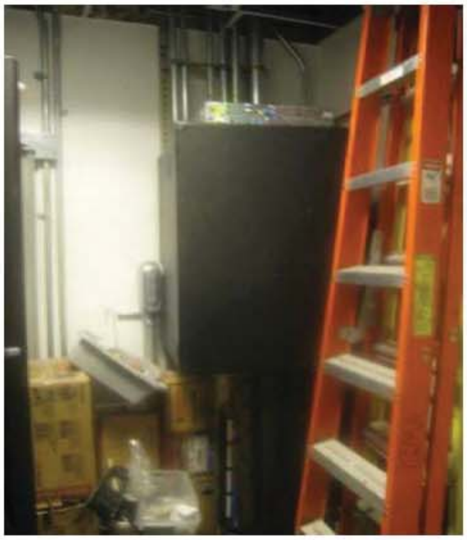


**Figure 4 -
Unlocked Communication Cabinet with Unsecured TSA Equipment**

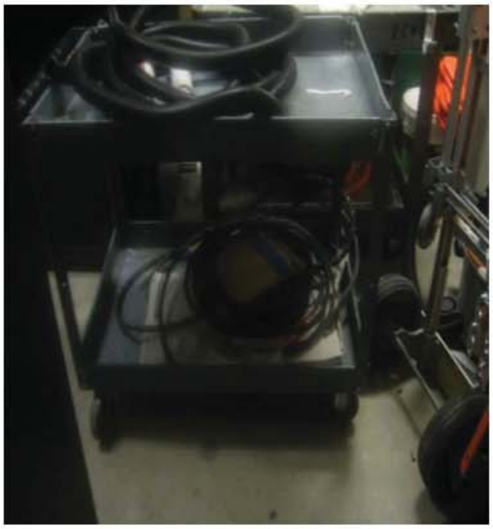


**Figure 5 -
Communication Room used as Storage**

Items being stored in the room were an obstruction and preventing access to the TSA IT equipment cabinets. A lack of housekeeping and maintenance caused a buildup of dust on TSA IT hardware stored within cabinets as shown in figure 6.

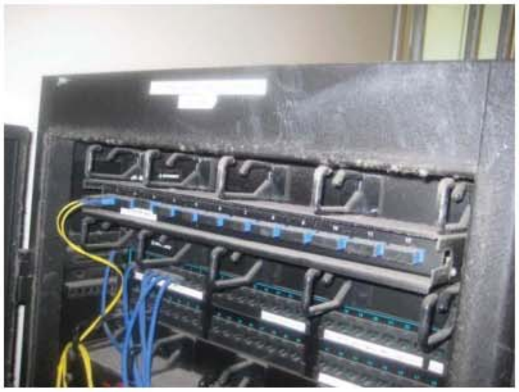


Figure 6- Dust covered Sensitive Equipment

According to DHS 4300A Sensitive Systems Handbook:

- Dusting of hardware and vacuuming of work area should be performed weekly with trash removal performed daily. Dust accumulation inside of monitors and computers is a hazard that can damage computer hardware.
- Cleaning supplies should not be stored inside the computer room.

Storage and housekeeping issues place the availability of TSA data at risk. Computer hardware damaged by dust and debris has the potential to cause delays for TSA's passenger and baggage screening processes.

Electronic Power Supply Protection

TSA did not have an operable uninterruptible power supply (UPS) in three communication cabinets. Figure 7 shows an unlocked cabinet and figure 8 shows inoperable UPS equipment.

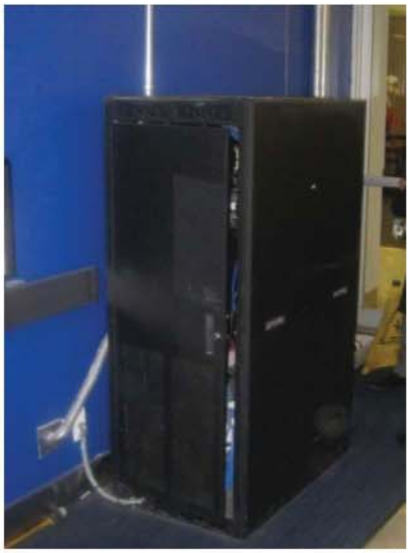


Figure 7-
Accessible Equipment

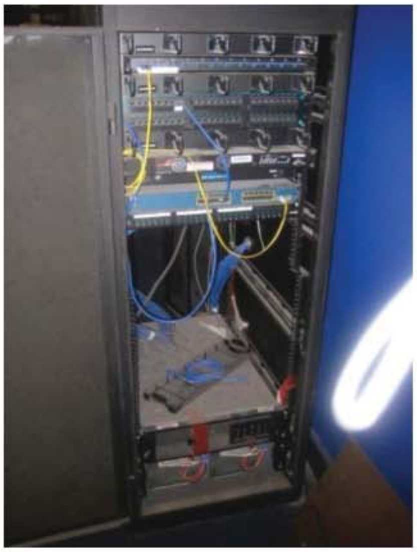


Figure 8-
Inoperable UPS

A sensitive equipment cabinet located in a public area was unlocked and left open to run an extension cord to a nearby electrical outlet for power. Upon closer inspection, we determined that the UPS was inoperable and not being used to provide backup power to IT equipment. Additionally, the attached extension cord prohibited the cabinet from closing and locking.

According to the *DHS 4300A Sensitive Systems Handbook*:

> Electrical power must be filtered through an UPS system for all servers and critical workstations and surge suppressing power strips used to protect all other computer equipment from power surges.

Electrical power supply vulnerabilities place TSA data availability at risk. For example, TSA servers that are not connected to a working UPS may not operate following a power outage.

Humidity and Temperature Controls

TSA did not have any device to measure humidity in the 21 server/switch rooms that we visited at JFK. Additionally, 13 out of the 21 server/switch rooms did not contain temperature sensors. Of the eight rooms that had temperature sensors, only two had temperature readings within the acceptable range established by DHS policy.

According to the *DHS 4300A Sensitive Systems Handbook*:

- Humidity should be at a level between 35 percent and 65 percent.
- Temperatures in computer storage areas should be between 60 and 70 degrees Fahrenheit.

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Technical Controls

TSA's implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, identified vulnerabilities on TSA servers at JFK had not been resolved or patched in a timely fashion.

Patch Management

In February 2014, we observed TSA staff scan two servers located at JFK for vulnerabilities. [redacted][2] Table 2 provides the number of vulnerabilities by server.

[2] Critical vulnerabilities should be addressed immediately due to the imminent threat to a network.

Table 2- Critical, High, and Medium Vulnerabilities

TSA Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]

According to *DHS Sensitive Systems Policy Directive 4300A*:

> Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.

Server vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of TSA data.

Management Controls

TSA's implementation of management controls for the Airport Authority's Security Systems operating at JFK did not conform fully to DHS policies. Specifically, TSA had not designated the Security System as a DHS IT system. As a result, TSA had not performed the applicable security authorization processes and privacy requirements over the surveillance system at JFK terminals.

CCTVs and Surveillance Systems

TSA did not designate the JFK CCTV cameras and surveillance system as DHS IT systems. As a result, the component did not implement the applicable, operational, technical, and managerial controls for the cameras and the systems. TSA officials stated that it was not responsible for the cameras and surveillance system because they belong to the Airport Authority.

However, TSA provided the funding for the JFK CCTV cameras and surveillance systems to the New York Airport Authority. The funding was an estimated $7.2 million to design, install, and maintain the JFK CCTV intrusion detection systems and other surveillance equipment. The Airport Authority Selected Surveillance Systems (Security System) includes CCTV cameras, detection systems, other surveillance hardware, storage equipment, and associated electrical cabling, and

support facilities monitored at JFK. The Airport Authority sets the conditions for shared use of these systems throughout JFK. Figure 9 shows the TSA's Security System.

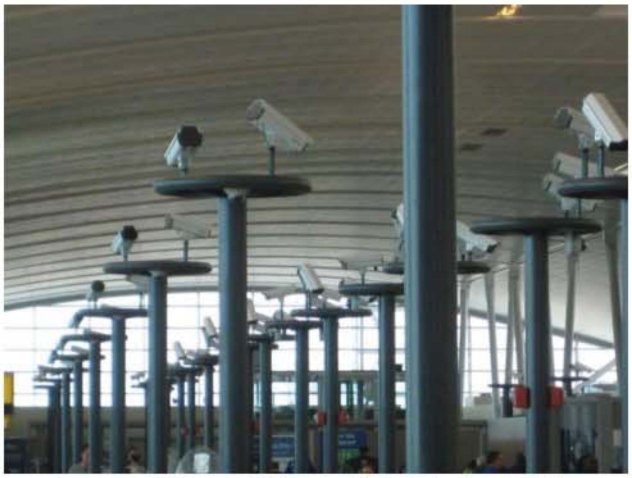


Figure 9-Security System at JFK

According to the agreement between the Airport Authority and TSA, the Security System provides greater surveillance of TSA areas to enhance security at JFK and assists in resolution of law enforcement issues. The Airport Authority is the owner of the Security System and is responsible for the repairs and maintenance. All media generated from the Security System remains with the Airport Authority. Although, the Airport Authority owns the systems, TSA controls the system design, identification of milestones, and who has allowable access to the system data. TSA officials also have unlimited ability to access information from the Security System to conduct TSA administrative or Top Secret criminal investigations.

The Security System collects images from all cameras to a video management system that stores the information for a minimum of 31 days. Since information that DHS uses is being stored, transmitted, and monitored on this system, and the Port Authority is operating this system on behalf of TSA, then TSA has the requirement to designate the Security System as a DHS IT system. However, TSA officials stated that because this system belongs to the Airport Authority it did

not need to conduct required security authorization processes, a privacy threshold analysis (PTA), or a privacy impact assessment (PIA).[3]

According to *DHS Sensitive Systems Policy Directive 4300A*:

> A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf.

DHS Sensitive Systems Policy Directive 4300A states that Component Chief Information Security Officers (CISO) shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

[3] A privacy threshold analysis is performed to determine if additional privacy compliance documentation is required, such as a privacy impact assessment. A privacy impact assessment is a publicly released assessment of the privacy impact of an information system and includes an analysis of the personally identified information collected, stored, and shared.

PII includes photographic facial images and any other unique identifying number or characteristic.

Also, Office of Management and Budget (OMB) M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when it uses IT to collect new information.

TSA has not fulfilled security authorization or privacy requirements for the cameras and surveillance systems at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put this information at risk, and lead to violations of U.S. privacy laws and DHS policy.

Recommendations

We recommend that the TSA Chief Information Officer (CIO):

Recommendation #1:

Comply with DHS policy concerning physical security, housekeeping and electronic power supply protection at all locations at JFK that contain TSA IT assets.

Recommendation #2:

Comply with DHS policy concerning fire protection at all locations at JFK that contain TSA IT assets.

Recommendation # 3:

Maintain JFK servers and network rooms free of excess storage that may cause damage to the equipment.

Recommendation #4:

Obtain humidity and temperature sensors for the JFK server rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Recommendation #5:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #6:

Designate the intrusion detection and surveillance Security Systems as DHS IT systems and implement applicable management, technical, operational, and privacy controls and reviews.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Assistant Director, Departmental Government Accountability Office (GAO) OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #1 through #5, but non-concurred with recommendation #6. Additionally, TSA has already taken actions and has submitted supporting documentation to resolve the reported deficiencies for recommendations #1, #3, and #5. We consider these recommendations resolved, but open pending verification of corrective and planned actions and supportive documentation.

Recommendation #1:

DHS concurred with recommendation 1. TSA officials recognize the need to comply with DHS policies on physical security, housekeeping, and electrical power supply protection by conducting quarterly cleaning of all IT equipment cabinets as well as ensuring that all uninterrupted power supplies are operational. TSA took several corrective actions and submitted supporting documentation. We agree that the steps TSA is taking, and plans to take, will satisfy this recommendation. Our recommendation will remain open and resolved until we receive and review supporting documentation for the corrective actions.

Recommendation #2:

DHS concurred with recommendation 2. TSA officals recognize the need to comply with the DHS policy concerning fire protection. TSA plans to take corrective actions to ensure that all locations at JFK that contain TSA IT assets are equipped with fire extinguishers. Additionally, TSA plans to verify the presence of other required fire protection equipment at all of its locations at JFK. TSA estimated that corrective actions would be completed by November 30, 2014.

We agree that the steps that TSA is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until we receive and review the corrective actions and supporting documentation.

Recommendation #3:

DHS concurred with recommendation 3. TSA's response outlines corrective actions for the removal of the excess items and the assurance to refrain from using IT equipment rooms as storage areas. We agree that the steps TSA is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until we receive and review the corrective actions and supporting documentation.

Recommendation #4:

DHS concurred with recommendation 4. TSA recognizes that temperature and humidity levels in computer storage areas should be between 60 and 70 degrees Fahrenheit and at a level between 35 percent and 65 percent, respectively. TSA plans to coordinate with facilities management to ensure that the Airport Authority complies with these requirements. TSA estimated that the corrective actions would be completed by October 31, 2014. We recognize these actions as positive steps and look forward to learning more about the continued progress in the future. This recommendation will remain open and resolved pending receipt and verification of planned actions and supporting documentation

Recommendation #5:

DHS concurred with recommendation 5. TSA stated that it remediated the identified vulnerabilities. TSA also stated that another subsequent security scan of the JFK servers was conducted to ensure vulnerabilities identified previously were no longer present on the servers. TSA provided supporting documentation for this recommendation. This recommendation will remain open and resolved pending verification of corrective actions and supporting documentation.

Recommendation #6:

DHS did not concur with recommendation 6. Instead of addressing directly our recommendation to designate detection and surveillance systems as DHS IT systems and to initiate appropriate IT security and privacy controls, TSA indicated it does not have a relationship at the JFK Airport that meets the definition of DHS 4300A Sensitive Systems Handbook for DHS IT systems. In TSA's

response, it stated that, because the intrusion detection and surveillance security systems are owned and operated by the Airport Authority, it had no responsibility to ensure that IT security and privacy controls were met.

According to the DHS Sensitive Systems Policy Directive 4300A, however, a DHS IT system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf. The systems at JFK transmit, store, and process data on behalf of DHS. Based on the Department's definition, these systems are IT systems and need to be treated as such by DHS. Because TSA has refused to define the detection and surveillance systems as DHS IT systems, TSA did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

We do not agree with DHS's response to this recommendation. The response does not provide for corrective actions to address the security and privacy concerns identified. DHS needs to perform security and privacy reviews of the surveillance systems at JFK airport. By not peforming these reviews, vulnerabilitilies may exist that may put the information collected at risk and lead to security breaches, and violations of DHS policy, and U.S. privacy laws. To assist in this process, we have added additional recommendations, #15 and #16, to our report that will need to be addressed before we can resolve the status of this recommendation.

We look forward to reviewing TSA's progress in the future. However, this recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

CBP Did Not Comply Fully with DHS Sensitive Systems Policies

CBP did not comply fully with DHS operational, technical, and management controls. Specifically, several CBP servers and telecommunication rooms did not contain humidity and temperatures sensors. Additionally, the temperature of several of the rooms reviewed with sensors had room temperatures that exceeded temperature ranges established by DHS policy. The humidity control readings for these rooms were within the ranges set by DHS policy. Also, CBP had an unlocked and open switch device in an open storage area allowing the potential for unauthorized access. In addition, CBP had not implemented known information security software patches to its servers at JFK. Finally, CBP did not designate the CCTV cameras and surveillance room as DHS IT systems nor did they implement the applicable, operational, technical, and managerial controls for these JFK systems. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by CBP at JFK.

Operational Controls

CBP server rooms and communication closets at JFK were clean and well maintained. However, onsite implementation of operational controls did not conform fully to DHS policies. For example, temperatures in CBP JFK server rooms were not within the temperature range recommended by the DHS 4300A Sensitive Systems Handbook. Additionally, one of the CBP sites did not have adequate equipment to prevent unauthorized access to CBP communication switches.

Humidity and Temperature Controls

Six out of 21 CBP switch rooms at JFK did not have humidity and temperature sensors. Five rooms with sensors had temperatures that exceeded temperature ranges established by DHS policy. The humidity control readings for these five rooms were within the ranges set by DHS policy.

According to the *DHS 4300A Sensitive Systems Handbook*:

- Humidity should be at a level between 35 percent and 65 percent.
- Temperatures in computer storage areas should be between 60 and 70 degrees Fahrenheit.

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Inadequate Equipment

CBP did not have a large enough box in the office storage area to contain one of its telecommunication switches. As a result, the box could not properly close. Figure 10 shows the box and the telecommunication switches mounted unprotected, beside the box.

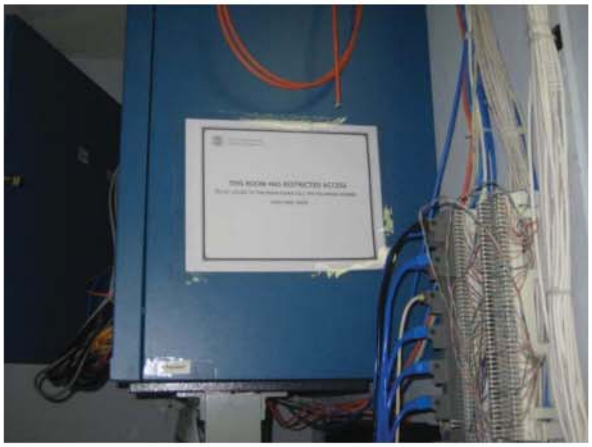


Figure 10- Unlocked Switch Box

According to DHS Sensitive System Policy Directive 4300A:

> Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.

Without adequate physical security controls, unauthorized individuals may gain access to sensitive TSA hardware.

Technical Controls

CBP's implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, identified vulnerabilities on CBP servers were not being resolved in a timely manner.

Patch Management

In February 2014, we observed CBP staff perform vulnerability scans on the three servers located at JFK. [redacted] Table 3 provides the number of vulnerabilities identified by server.

Table 3- Critical, High, and Medium Vulnerabilities

CBP Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]

According to the *DHS 4300A Sensitive Systems Handbook*:

> Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction stated in the Information Security Vulnerability Management message published by the DHS Security Operations Center.

Server vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of CBP data. CBP IT Security officials reviewed the technical results for the three servers and immediately began corrective actions to resolve the two critical vulnerabilities.

Management Controls

CBP's implementation of management controls for the CCTV cameras and surveillance room systems operating at JFK did not conform fully to DHS policies. For example, CBP had not designated the CCTV cameras and surveillance room systems as DHS IT systems. As a result, CBP had not performed the security authorization processes and privacy requirements over the newly installed physical security measures at JFK terminals.

CCTV Cameras and Surveillance Room

CBP did not designate the JFK CCTV cameras and surveillance monitoring room systems as DHS IT systems nor did it implement the applicable, operational, technical, and managerial controls for these JFK systems. CBP failed to designate the cameras and surveillance monitoring room equipment as DHS IT systems, as required by *DHS Sensitive Systems Policy Directive 4300A,* sections 1.4.7 and 1.4.8.

We observed several CCTV cameras in the Terminal 4 area of the CBP passenger processing primary and secondary locations.[4] Figure 11 shows CBP's primary passenger processing area.

[4] Primary processing is the first point of examination of passengers by a CBP officer. Those passengers selected for further examination are referred to a secondary processing point for a more thorough inspection.

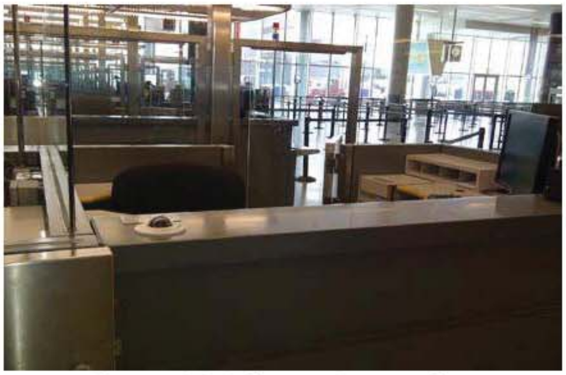


Figure 11-Primary Processing

In 2013, CBP acquired newly renovated space at JFK that included CCTV cameras and a CBP surveillance monitoring room containing IT equipment. The CBP Command and Control Center employees use the cameras to assess threats signaled by alarm events and for surveillance by CBP airport security to monitor activity both inside and outside the terminal.[5] CBP requires a secondary CCTV system that allows officers to monitor detainees in the secondary processing areas, interview rooms, holding rooms, and expedited voluntary removal rooms. CBP officials estimate that approximately 300 cameras are throughout viewable areas within CBP primary passenger processing, secondary passenger processing, interview rooms, and holding rooms. CBP officials operate and monitor the cameras from a CBP secured surveillance monitoring room. Only CBP officials have permission to view cameras observing operations in secondary processing areas. Figure 12 shows the CBP surveillance monitoring room.

[5] Command and Control Center is a station centrally located within the airport's Federal Inspection Service Areas, where CBP systems are monitored.

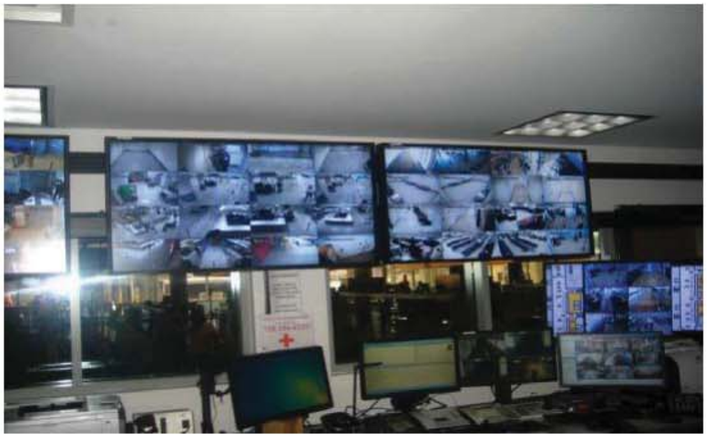


Figure 12- Views of CBP Surveillance Monitoring

The cameras record audio and visual interactions between CBP officers and passengers. However, the Airport Authority owns the CCTV cameras. Since CBP information is being stored, transmitted, and monitored on this system, CBP has the requirement to designate the cameras and surveillance monitoring room as DHS IT systems. By not designating the cameras and surveillance monitoring room as an IT system, CBP did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A.

According to *DHS Sensitive Systems Policy Directive 4300A*:

> A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf.

DHS Sensitive Systems Policy Directive 4300A states that the CISO shall ensure that all information systems are formally assessed through a comprehensive evaluation of management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates PII. Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The

PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

PII includes photographic facial images and any other unique identifying number or characteristic.

Among other things, OMB M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when it uses IT to collect new information.

CBP has not fulfilled security authorization or privacy requirements for the cameras and surveillance equipment at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put the information at risk, and may lead to violations of U.S. privacy laws and DHS policy.

Recommendations:

We recommend that the CBP CIO

Recommendation #7:

Maintain the temperatures of servers and switch rooms within the established temperature ranges.

Recommendation #8:

Secure CBP information technology equipment from unauthorized access.

Recommendation #9:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #10:

Designate the surveillance systems as CBP/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS GAO OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #7 through #10 and has provided details on corrective actions to address each recommendation.

Recommendation #7:

DHS concurred with recommendation 7. CBP's response outlines its plans to install humidity and temperatures sensors. CBP agrees to set humidity and temperatures to the recommended range per the DHS 4300A Sensitive Systems Handbook. These corrective actions are expected to be completed by December 31, 2014. We believe that such efforts are good steps toward addressing our recommendation. We look forward to receiving additional documentation on CBP's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #8:

DHS concurred with recommendation 8. CBP's response outlines its plans to obtain a lockable rack large enough to secure the identified telecommunication switch from unauthorized access. This corrective action is expected to be completed by January 31, 2015. We look forward to receiving notification from

CBP that the lockable rack has been installed and in use. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #9:

DHS concurred with recommendation 9. CBP officials plan to review the OIG reported vulnerabilities to ensure that all critical and high vulnerabilities are addressed. CBP's review is expected to be completed by February 28, 2015. Although, this response appears to address critical and high vulnerabilities, it does not address any corrective actions for the remaining vulnerabilities identified in our report. We look forward to learning more about CBP's actions on this recommendation in the near future. This recommendation will remain open and unresolved pending verification of corrective actions and supporting documentation for all vulnerabilities identified.

Recommendation #10:

Although DHS concurred with recommendation 10, it does not appear that its concurrence addressed all of the concerns noted in our recommendation. Specifically, CBP does not take full ownership of all of the CCTV cameras. CBP agrees that it needs to perform a PTA for CBP's collection and use of the CCTV information. Additionally, CBP plans to determine whether further privacy compliance coverage is warranted through an update to DHS/CBP's current CCTV PIA.

However, CBP only plans to perform the PTA and PIA on the cameras it owns. Although the Port Authority owns some of the cameras in CBP's areas, these cameras and surveillance systems also store, transmit, and monitor CBP information. As a result, CBP has the requirement to designate the cameras and surveillance monitoring room systems as DHS IT systems and to perform required security and privacy reviews. By not designating the cameras and surveillance monitoring room systems as a DHS IT system, CBP did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

DHS/CBP did not provide sufficient corrective actions for our review. We look forward to reviewing CBP's progress in the future. However, this recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

ICE Did Not Comply Fully with DHS Sensitive Systems Policies

ICE did not comply fully with DHS operational, technical and management policies for its servers and switches operating at JFK. Specifically, ICE server and telecommunication rooms did not contain humidity and temperature sensors. Also, ICE had not implemented identified information security patches to its servers. Additionally, ICE did not designate the CCTV cameras and surveillance monitoring equipment as DHS IT systems nor did it implement the applicable, operational, technical, and managerial controls for these JFK systems. Finally, ICE CCTV cameras and surveillance system did not function properly or reliably. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by ICE at JFK.

Operational Controls

ICE server rooms and communications closets at JFK were clean and well maintained. However, onsite implementation of operations controls did not conform fully to DHS policies. For example, the ICE servers and switch rooms did not have the appropriate humidity and temperature control devices to measure and record humidity and temperature ranges as required by DHS policies.

Humidity and Temperature Controls

The ICE servers and switch rooms did not contain any humidity and temperature sensors.

According to the *DHS 4300A Sensitive Systems Handbook*:

- Humidity should be at a level between 35 percent and 65 percent.
- Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit.

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Technical Controls

Patch Management

ICE implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, vulnerabilities identified on ICE servers were not being resolved in a timely fashion. Table 4 provides the number of critical, high, and medium level vulnerabilities identified for each server.

Table 4- Critical, High, and Medium Vulnerabilities

ICE Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	0	1	6
2	0	2	4
3	0	0	2
4	0	1	2
Total	0	4	14

According to the DHS 4300A Sensitive Systems Handbook:

> Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction as stated in the Information Security Vulnerability Management message published by the DHS Security Operations Center.

Server vulnerabilities that are not mitigated could compromise the confidentiality, integrity, and availability of ICE data. If the identified security vulnerabilities are not addressed, they could lead to the introduction of malicious code or unauthorized access to ICE information systems.

Management Controls

CCTV and Surveillance Systems

ICE's implementation of management controls over its CCTV cameras and surveillance systems for the physical security requirements at JFK did not conform fully to DHS policies. Specifically, in April 2010, ICE acquired space at Terminal 4, JFK for the Joint Narcotics and Smuggling Unit. This space includes CCTV cameras, a surveillance monitor, and a digital video receiver. Figure 13 shows the ICE surveillance monitor.

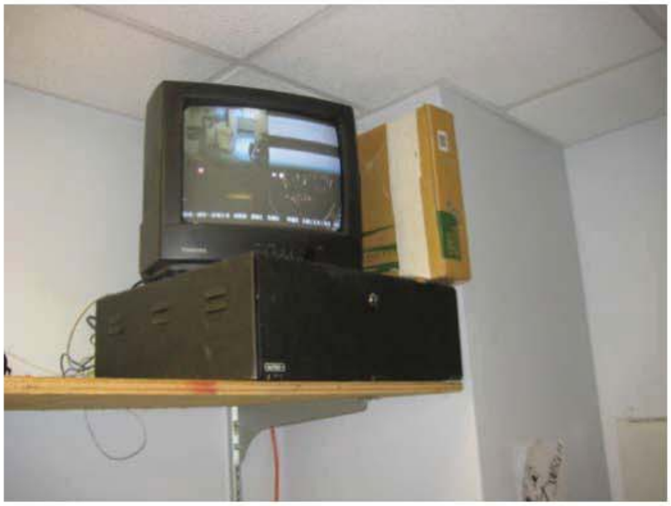


Figure 13- ICE's Surveillance Monitor

However, ICE failed to designate the cameras and surveillance monitor as a DHS IT system as required by *DHS Sensitive Systems Policy Directive 4300A,* sections 1.4.7 and 1.4.8.

ICE officials stated that they did not designate the cameras and surveillance monitor as a DHS IT system because the Airport Authority owned the system. Since ICE information is being stored, transmitted, and monitored on this system, then ICE has the requirement to designate the cameras and surveillance monitor as a DHS IT system. By not designating the cameras and surveillance monitoring room systems as a DHS IT system, ICE did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming

these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

Additionally, two of four CCTV cameras at the Terminal 4 Joint Narcotics and Smuggling Unit communication room were not working during our site visit. The surveillance system monitor connected to the CCTV cameras did not properly display all captured images. ICE officials stated that the cameras had not worked for a period of time but the surveillance system monitor was operating properly 3 days prior to our visit. The ICE officials indicated that they would request camera repairs.

According to *DHS Sensitive Systems Policy Directive 4300A*:

> A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf.

DHS Sensitive Systems Policy Directive 4300A states that the CISO shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates PII. Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

PII includes photographic facial images and any other unique identifying number or characteristic.

Also, OMB M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when they use IT to collect new information.

ICE has not fulfilled security authorization or privacy requirements for the cameras and surveillance equipment at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put the information at risk, and lead to violations of U.S. privacy laws and DHS policy.

Lastly, the identified vulnerabilities on ICE CCTV cameras and surveillance monitor degrade physical security for ICE and law enforcement staff members.

Recommendations

We recommend that the ICE CIO:

Recommendation #11:

Obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Recommendation #12:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #13:

Designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Recommendation #14:

Upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit at JFK.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS GAO OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #11 through #14 and has already taken actions to resolve reported deficiencies.

Recommendation #11:

DHS concurred with recommendation 11. The ICE OCIO plans to to obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300A Sensitive Systems Handbook. ICE estimated the corrective actions would be completed by October 31, 2014. We look forward to receiving additional documentation on ICE's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #12:

DHS concurred with recommendation 12. The ICE OCIO plans to remediate vulnerabilities as they are identified, or within timeframes specified by the DHS Security Operations Center messages. ICE expects this process to be an ongoing effort, however, with an estimated completion date of December 31, 2014. We look forward to receiving additional documentation on ICE's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #13:

DHS concurred with recommendation 13. ICE agreed with the intent of this recommendation for the the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ICE's OCIO and Homeland Security Investigations plans to coordinate and designate the surveillance systems as ICE/DHS IT systems. ICE also plans to implement applicable DHS management, technical, operational controls, and privacy controls and reviews. ICE anticipates completing corrective actions for this recommendation by June 30, 2015. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #14:

DHS concurred with recommendation 14. ICE's Homeland Security Investigations, with assistance from the ICE OCIO, plans to assess the feasibility to upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ICE officials estimate the completion date of the feasibility study by June 30, 2015. Although this response addresses part our recommendation, it does not outline any corrective actions for the repair of the inoperable CCTV cameras and surveillance system. We look forward to reviewing ICE's progress in the future. This recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

USSS Fully Complied with DHS Sensitive Systems Policies

USSS fully complied with DHS operational, technical, and management operational policies for its telecommunication room at JFK. We audited IT security controls of the USSS telecommunication room located at the JFK on-site building number 75. This location had a DHS OneNet connection and a network switch device. The telecommunications room was clean and well maintained. Visitor's logs were also maintained. Humidity and temperature sensor readings were within DHS policy guidelines. Since, the JFK location did not have an on-site server, vulnerability scans were not applicable.

Department's Nonconcurrence

Based on the Department's nonconcurrence with recommendation #6, we have added two additional recommendations that were not part of our draft report. Specifically, we recommend that the DHS CIO:

Recommendation #15:

Coordinate steps with DHS components located at JFK, to ensure their compliance with DHS Sensitive Systems Policy Directive 4300A, Section 1.4.8, and to designate the JFK CCTV cameras and surveillance systems as DHS IT systems.

We also recommend that the DHS Chief Privacy Officer:

Recommendation #16:

Require DHS components located at JFK to prepare PTAs and, as applicable, PIAs for the JFK CCTV cameras and surveillance systems as directed by privacy laws and policy.

Appendix A
Objectives, Scope, and Methodology

The DHS Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

This audit is part of a program to evaluate, on an ongoing basis, the implementation of DHS technical and information security policies and procedures at DHS sites. The objective of this program is to determine the extent to which critical DHS sites comply with the Department's technical and information security policies and procedures, according to *DHS Sensitive Systems Policy Directive 4300A* and its companion document, the *DHS 4300A Sensitive Systems Handbook*. Our primary focus was on evaluating the security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS IT infrastructure at this site. For example, we recorded humidity and temperature at different locations in the server rooms, and then averaged these readings. We also recorded humidity and temperature readings obtained from component sensors that existed in the rooms during fieldwork. We then compared these readings with DHS guidance.

We coordinated the implementation of this technical security evaluation program with the DHS Chief Information Security Officer. We interviewed TSA, CBP, ICE, and USSS, and other staff. We conducted site visits of TSA, CBP, ICE, and USSS facilities at and near JFK. We compared the DHS IT infrastructure that we observed onsite with the documented standards provided by the auditees.

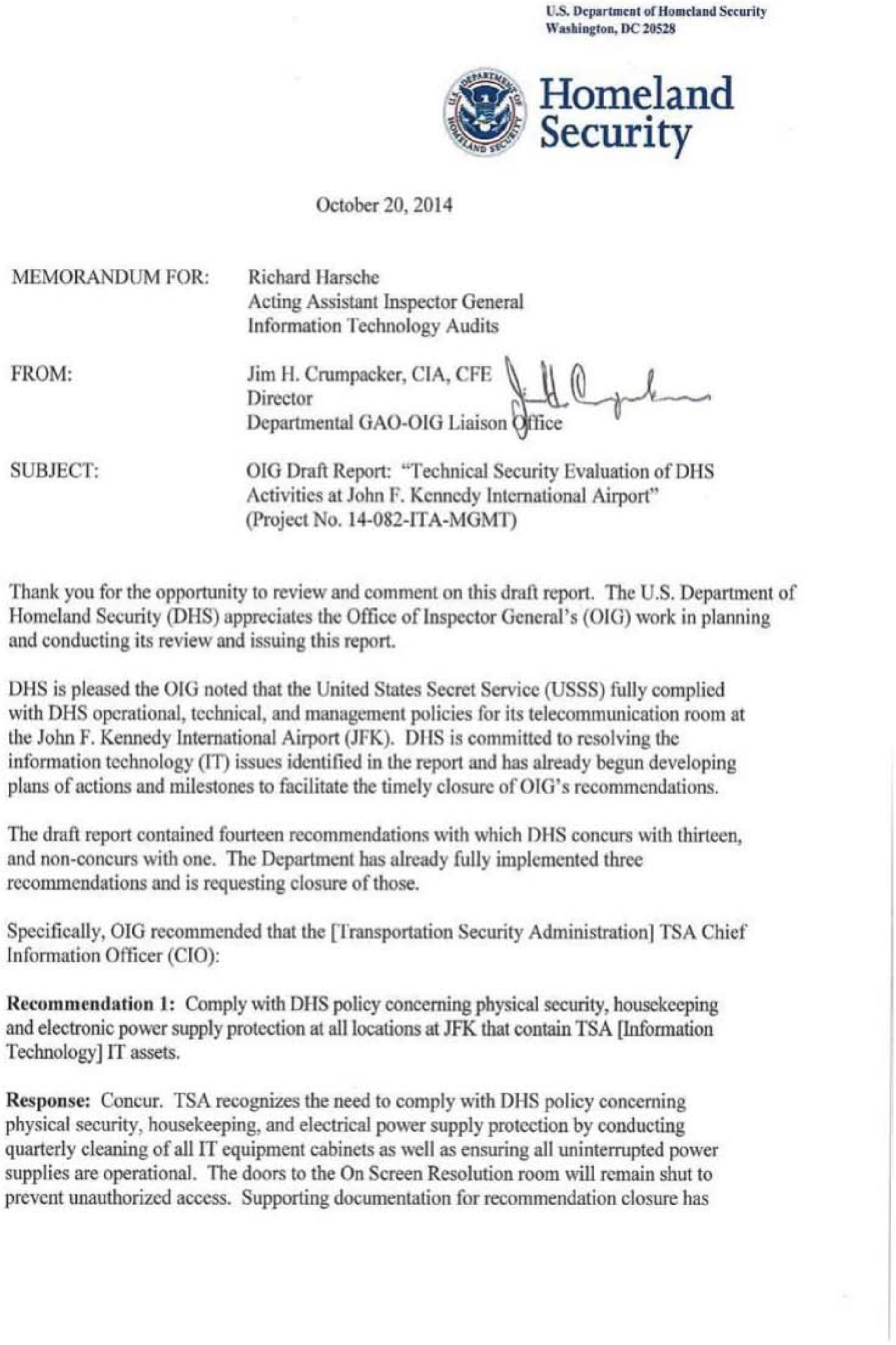
We reviewed the Information Assurance Compliance System documentation, such as the authority-to-operate letter, contingency plans, and system security plans. Additionally, we reviewed guidance provided by DHS to its components in the areas of system documentation, patch management, and wireless security. We also reviewed applicable DHS and components' policies and procedures, as well as Government-wide guidance. We gave briefings and presentations to DHS staff concerning the results of fieldwork and the information summarized in this report.

We conducted this performance audit between November 2013 and April 2014 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable

basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

We appreciate the efforts of DHS management and staff to provide the information and access necessary to accomplish this audit. The principal OIG points of contact for the audit are Richard Harsche, Acting Assistant Inspector General for Information Technology Audits, (202) 254-4100, and Sharon Huiswoud, Director, Information Systems Division, (202) 254-5451. Appendix D contains a major OIG contributors listing.

Appendix B
Management Comments to the Draft Report



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

October 20, 2014

MEMORANDUM FOR:	Richard Harsche Acting Assistant Inspector General Information Technology Audits
FROM:	Jim H. Crumpacker, CIA, CFE Director Departmental GAO-OIG Liaison Office
SUBJECT:	OIG Draft Report: "Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport" (Project No. 14-082-ITA-MGMT)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG) work in planning and conducting its review and issuing this report.

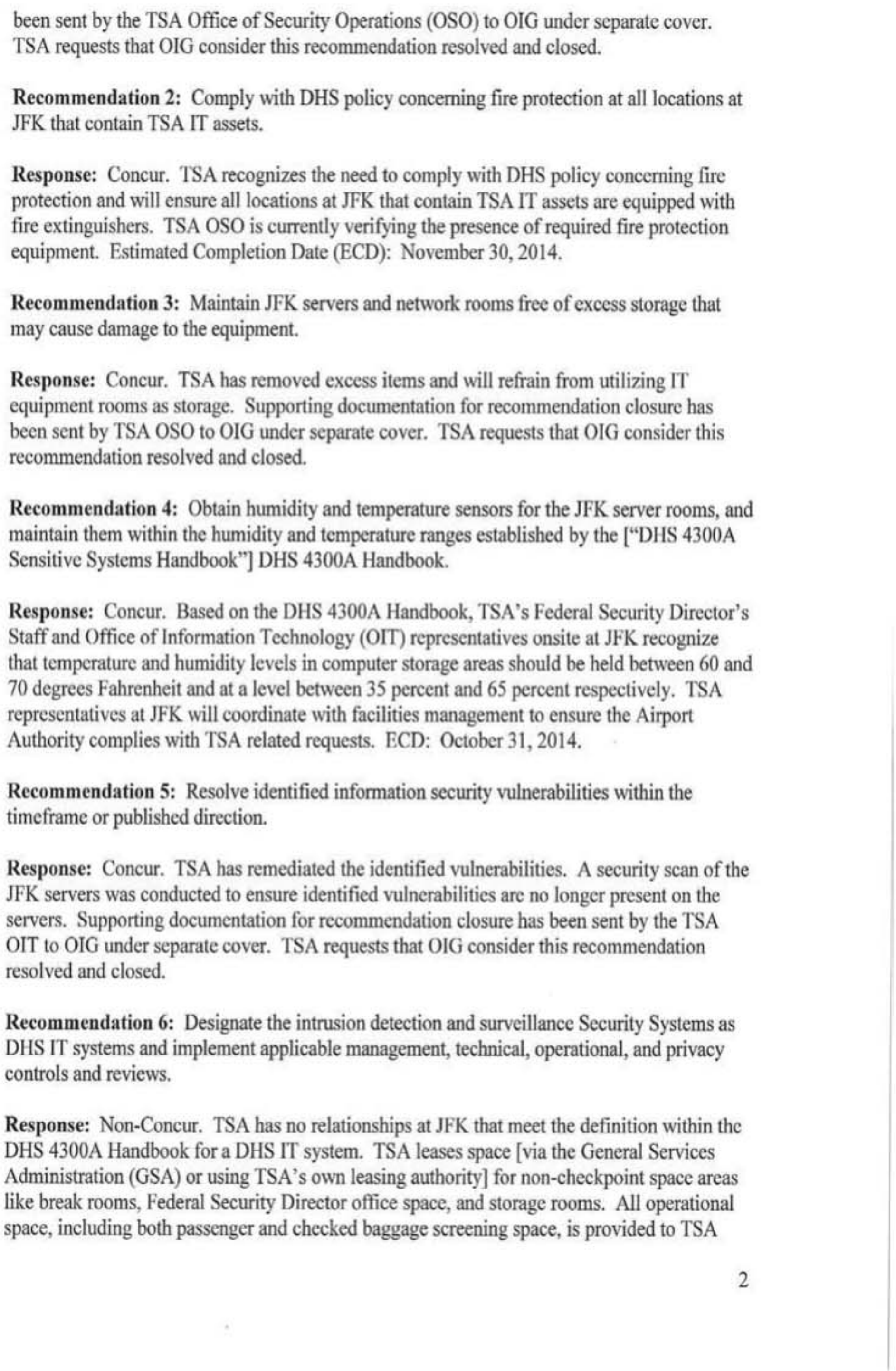
DHS is pleased the OIG noted that the United States Secret Service (USSS) fully complied with DHS operational, technical, and management policies for its telecommunication room at the John F. Kennedy International Airport (JFK). DHS is committed to resolving the information technology (IT) issues identified in the report and has already begun developing plans of actions and milestones to facilitate the timely closure of OIG's recommendations.

The draft report contained fourteen recommendations with which DHS concurs with thirteen, and non-concurs with one. The Department has already fully implemented three recommendations and is requesting closure of those.

Specifically, OIG recommended that the [Transportation Security Administration] TSA Chief Information Officer (CIO):

Recommendation 1: Comply with DHS policy concerning physical security, housekeeping and electronic power supply protection at all locations at JFK that contain TSA [Information Technology] IT assets.

Response: Concur. TSA recognizes the need to comply with DHS policy concerning physical security, housekeeping, and electrical power supply protection by conducting quarterly cleaning of all IT equipment cabinets as well as ensuring all uninterrupted power supplies are operational. The doors to the On Screen Resolution room will remain shut to prevent unauthorized access. Supporting documentation for recommendation closure has



been sent by the TSA Office of Security Operations (OSO) to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 2: Comply with DHS policy concerning fire protection at all locations at JFK that contain TSA IT assets.

Response: Concur. TSA recognizes the need to comply with DHS policy concerning fire protection and will ensure all locations at JFK that contain TSA IT assets are equipped with fire extinguishers. TSA OSO is currently verifying the presence of required fire protection equipment. Estimated Completion Date (ECD): November 30, 2014.

Recommendation 3: Maintain JFK servers and network rooms free of excess storage that may cause damage to the equipment.

Response: Concur. TSA has removed excess items and will refrain from utilizing IT equipment rooms as storage. Supporting documentation for recommendation closure has been sent by TSA OSO to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 4: Obtain humidity and temperature sensors for the JFK server rooms, and maintain them within the humidity and temperature ranges established by the ["DHS 4300A Sensitive Systems Handbook"] DHS 4300A Handbook.

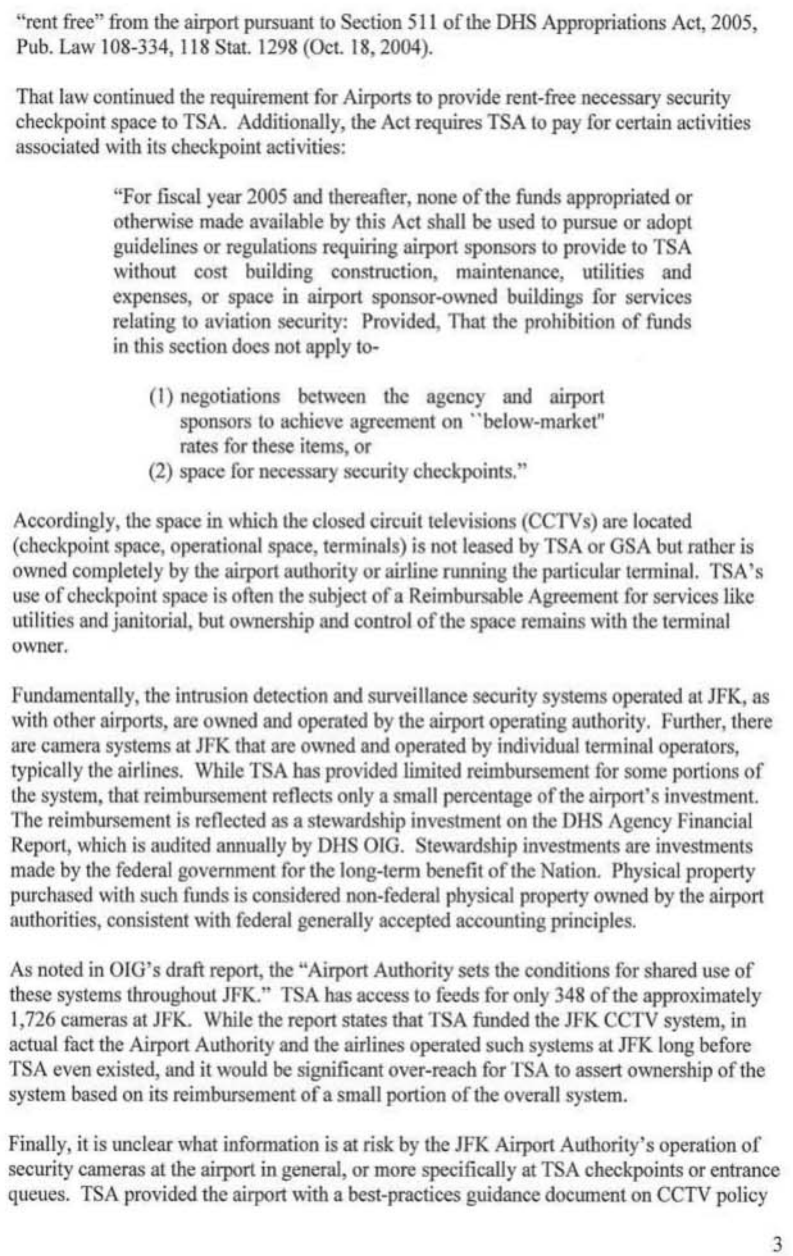
Response: Concur. Based on the DHS 4300A Handbook, TSA's Federal Security Director's Staff and Office of Information Technology (OIT) representatives onsite at JFK recognize that temperature and humidity levels in computer storage areas should be held between 60 and 70 degrees Fahrenheit and at a level between 35 percent and 65 percent respectively. TSA representatives at JFK will coordinate with facilities management to ensure the Airport Authority complies with TSA related requests. ECD: October 31, 2014.

Recommendation 5: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. TSA has remediated the identified vulnerabilities. A security scan of the JFK servers was conducted to ensure identified vulnerabilities are no longer present on the servers. Supporting documentation for recommendation closure has been sent by the TSA OIT to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 6: Designate the intrusion detection and surveillance Security Systems as DHS IT systems and implement applicable management, technical, operational, and privacy controls and reviews.

Response: Non-Concur. TSA has no relationships at JFK that meet the definition within the DHS 4300A Handbook for a DHS IT system. TSA leases space [via the General Services Administration (GSA) or using TSA's own leasing authority] for non-checkpoint space areas like break rooms, Federal Security Director office space, and storage rooms. All operational space, including both passenger and checked baggage screening space, is provided to TSA



"rent free" from the airport pursuant to Section 511 of the DHS Appropriations Act, 2005, Pub. Law 108-334, 118 Stat. 1298 (Oct. 18, 2004).

That law continued the requirement for Airports to provide rent-free necessary security checkpoint space to TSA. Additionally, the Act requires TSA to pay for certain activities associated with its checkpoint activities:

> "For fiscal year 2005 and thereafter, none of the funds appropriated or otherwise made available by this Act shall be used to pursue or adopt guidelines or regulations requiring airport sponsors to provide to TSA without cost building construction, maintenance, utilities and expenses, or space in airport sponsor-owned buildings for services relating to aviation security: Provided, That the prohibition of funds in this section does not apply to-
>
> (1) negotiations between the agency and airport sponsors to achieve agreement on ``below-market" rates for these items, or
> (2) space for necessary security checkpoints."

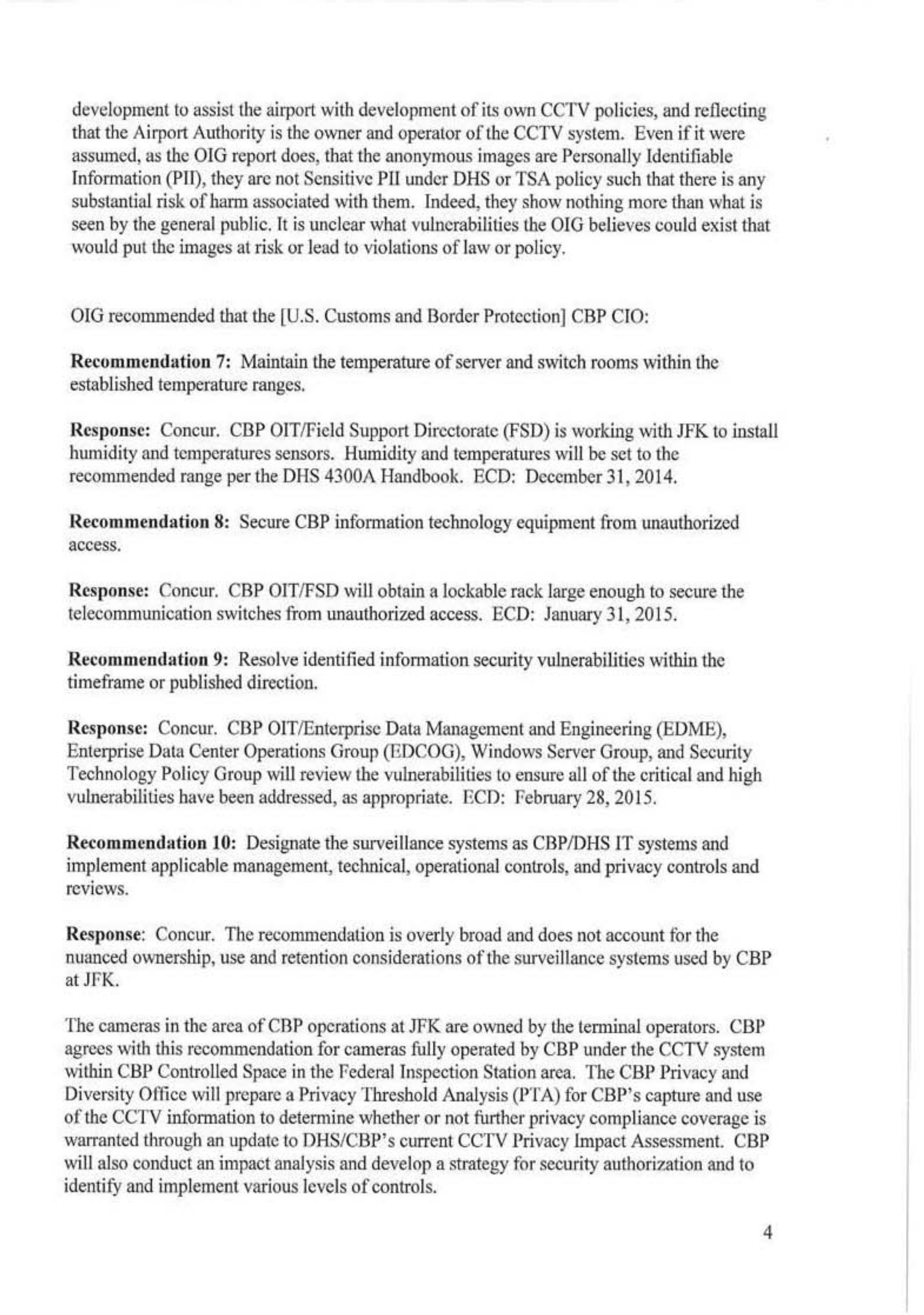
Accordingly, the space in which the closed circuit televisions (CCTVs) are located (checkpoint space, operational space, terminals) is not leased by TSA or GSA but rather is owned completely by the airport authority or airline running the particular terminal. TSA's use of checkpoint space is often the subject of a Reimbursable Agreement for services like utilities and janitorial, but ownership and control of the space remains with the terminal owner.

Fundamentally, the intrusion detection and surveillance security systems operated at JFK, as with other airports, are owned and operated by the airport operating authority. Further, there are camera systems at JFK that are owned and operated by individual terminal operators, typically the airlines. While TSA has provided limited reimbursement for some portions of the system, that reimbursement reflects only a small percentage of the airport's investment. The reimbursement is reflected as a stewardship investment on the DHS Agency Financial Report, which is audited annually by DHS OIG. Stewardship investments are investments made by the federal government for the long-term benefit of the Nation. Physical property purchased with such funds is considered non-federal physical property owned by the airport authorities, consistent with federal generally accepted accounting principles.

As noted in OIG's draft report, the "Airport Authority sets the conditions for shared use of these systems throughout JFK." TSA has access to feeds for only 348 of the approximately 1,726 cameras at JFK. While the report states that TSA funded the JFK CCTV system, in actual fact the Airport Authority and the airlines operated such systems at JFK long before TSA even existed, and it would be significant over-reach for TSA to assert ownership of the system based on its reimbursement of a small portion of the overall system.

Finally, it is unclear what information is at risk by the JFK Airport Authority's operation of security cameras at the airport in general, or more specifically at TSA checkpoints or entrance queues. TSA provided the airport with a best-practices guidance document on CCTV policy

3



development to assist the airport with development of its own CCTV policies, and reflecting that the Airport Authority is the owner and operator of the CCTV system. Even if it were assumed, as the OIG report does, that the anonymous images are Personally Identifiable Information (PII), they are not Sensitive PII under DHS or TSA policy such that there is any substantial risk of harm associated with them. Indeed, they show nothing more than what is seen by the general public. It is unclear what vulnerabilities the OIG believes could exist that would put the images at risk or lead to violations of law or policy.

OIG recommended that the [U.S. Customs and Border Protection] CBP CIO:

Recommendation 7: Maintain the temperature of server and switch rooms within the established temperature ranges.

Response: Concur. CBP OIT/Field Support Directorate (FSD) is working with JFK to install humidity and temperatures sensors. Humidity and temperatures will be set to the recommended range per the DHS 4300A Handbook. ECD: December 31, 2014.

Recommendation 8: Secure CBP information technology equipment from unauthorized access.

Response: Concur. CBP OIT/FSD will obtain a lockable rack large enough to secure the telecommunication switches from unauthorized access. ECD: January 31, 2015.

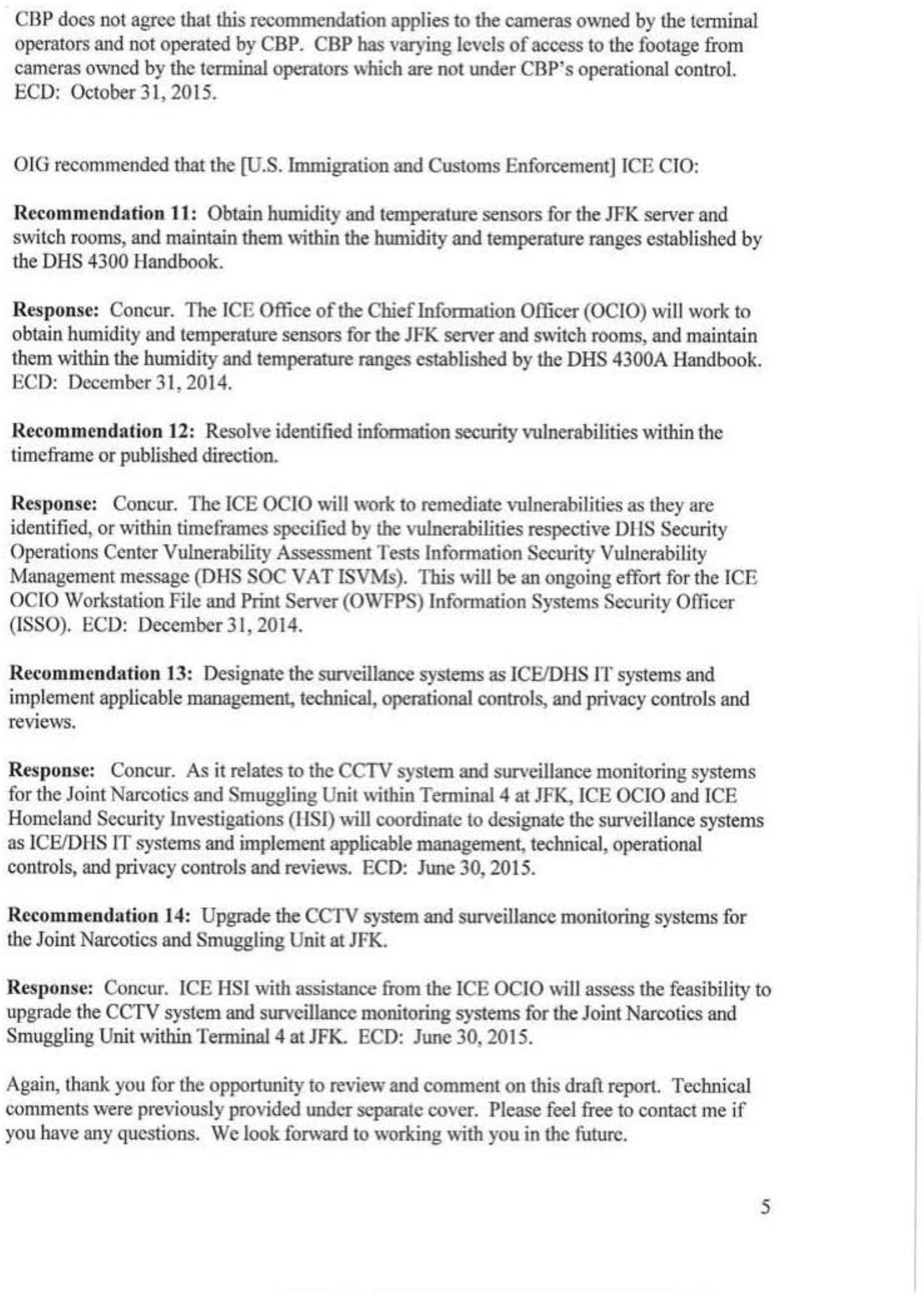
Recommendation 9: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. CBP OIT/Enterprise Data Management and Engineering (EDME), Enterprise Data Center Operations Group (EDCOG), Windows Server Group, and Security Technology Policy Group will review the vulnerabilities to ensure all of the critical and high vulnerabilities have been addressed, as appropriate. ECD: February 28, 2015.

Recommendation 10: Designate the surveillance systems as CBP/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Response: Concur. The recommendation is overly broad and does not account for the nuanced ownership, use and retention considerations of the surveillance systems used by CBP at JFK.

The cameras in the area of CBP operations at JFK are owned by the terminal operators. CBP agrees with this recommendation for cameras fully operated by CBP under the CCTV system within CBP Controlled Space in the Federal Inspection Station area. The CBP Privacy and Diversity Office will prepare a Privacy Threshold Analysis (PTA) for CBP's capture and use of the CCTV information to determine whether or not further privacy compliance coverage is warranted through an update to DHS/CBP's current CCTV Privacy Impact Assessment. CBP will also conduct an impact analysis and develop a strategy for security authorization and to identify and implement various levels of controls.



CBP does not agree that this recommendation applies to the cameras owned by the terminal operators and not operated by CBP. CBP has varying levels of access to the footage from cameras owned by the terminal operators which are not under CBP's operational control. ECD: October 31, 2015.

OIG recommended that the [U.S. Immigration and Customs Enforcement] ICE CIO:

Recommendation 11: Obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Response: Concur. The ICE Office of the Chief Information Officer (OCIO) will work to obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300A Handbook. ECD: December 31, 2014.

Recommendation 12: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. The ICE OCIO will work to remediate vulnerabilities as they are identified, or within timeframes specified by the vulnerabilities respective DHS Security Operations Center Vulnerability Assessment Tests Information Security Vulnerability Management message (DHS SOC VAT ISVMs). This will be an ongoing effort for the ICE OCIO Workstation File and Print Server (OWFPS) Information Systems Security Officer (ISSO). ECD: December 31, 2014.

Recommendation 13: Designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Response: Concur. As it relates to the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK, ICE OCIO and ICE Homeland Security Investigations (HSI) will coordinate to designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews. ECD: June 30, 2015.

Recommendation 14: Upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit at JFK.

Response: Concur. ICE HSI with assistance from the ICE OCIO will assess the feasibility to upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ECD: June 30, 2015.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

5

Appendix C
DHS Activities at JFK Airport

Transportation Security Administration

TSA uses technology to screen passengers and baggage on all departing flights at each of the JFK terminals and to support operation management at nearby office buildings.

We audited IT security controls at the following TSA locations:

- JFK Terminals 1, 2, 4, 5, 7, and 8,
- Office of the Federal Security Director, Jamaica, NY, and
- Office of Federal Air Marshal Service (FAMS), Jamaica, NY.

TSA staff at these locations use the following systems:

- Federal Air Marshal Service Network (FAMSNet) – provides the IT infrastructure to support the FAMS law enforcement mission to help detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews. FAMSNet provides Internet access as well as internal access to FAMS information systems including, but not limited to, email, databases, file sharing, printing, and a number of critical administrative and enforcement related programs. FAMSNet also provides a communication pathway to third-party and Government networks, such as those used by other DHS components, the Federal Aviation Administration, and other State and local law enforcement entities.
- Infrastructure Core System – provides electronic file and print capabilities to the entire TSA user community.
- TSA End User Computing System – provides TSA employees and contractors with desktops, laptops, local printers, mobile devices and other end user computing applications.
- Security Technology Integrated Program – combines many different types of components, including transportation security equipment, servers and storage, software/application products, and databases. Users physically access the transportation security equipment to perform screening or other administrative

functions. TSA's Office of Security Capabilities is the owner of the Security Technology Integrated Program.

- Transportation Security Administration Network (TSANet) – provides connectivity in airports for TSA users. TSANet consists of a geographically-dispersed wide area network and each site's local area network. The networks are connected to the DHS One Network (OneNet) and have been designated a mission essential system.

U.S. Customs and Border Protection

CBP employs over 1,600 staff at JFK to protect the United States from drug and human smugglers, agricultural diseases and pests, and terrorists. CBP personnel also:

- review flight data for terrorist-related activities,
- collect duties, and
- assess fines and civil penalties.

Also, CBP staff at nearby locations use IT assets to perform cargo and outbound passenger review and targeting. In addition, JFK CBP employees operate and maintain the international mail facility.

We audited IT security controls at the following CBP locations:

- JFK Terminals 1, 4, 5, 7, and 8, and
- CBP buildings Number 77 and 250, located in Jamaica, NY.

CBP staff at these locations use the following systems:

- Northeast Field Local Area Network – provides the general support network infrastructure for DHS/CBP users and electronic communications tools, which enables the execution of official duties. The Northeast Field Local Area Network includes 290 geographically dispersed sites using 9,000 devices connected to the OneNet to provide application services to CBP field offices.

- CBP Network Operations Center – maintains the performance, management, and administration of the core network and underlying supporting environment at CBP field site locations. In addition, the center deploys and maintains a network management system and a suite of network devices that collect and report real-time network security information. Further, the center manages the flow of information within interconnected systems in accordance with DHS Sensitive Security Policy.

- Windows 7 PC Client 6.1 – used as the Windows 7 standard desktop image for CBP workstations. Windows 7 PC Client 6.1 consists of a set of standard configurations and installs application software and configures systems according to DHS and CBP technical standards.

- The Windows File and Print System – provides CBP with file and printing services using the Microsoft Windows Server 2008 x 64 platforms.

- Treasury Enforcement Communication System (TECS) – supports enforcement and inspection operations for several components of DHS and is a vital tool for local, State, tribal, and Federal Government law enforcement and intelligence communities.6 TECS includes several subsystems for enforcement, inspection, and intelligence records relevant to the antiterrorist and law enforcement mission of CBP and other Federal agencies.

[6] Formerly known as the Treasury Enforcement Communications System, TECS is no longer an acronym (effective December 19, 2008) and is principally owned and managed by CBP.

U.S. Immigration and Customs Enforcement

The New York ICE Office of the Special Agent in Charge is responsible for the administration and management of all investigative and enforcement activities within its geographical boundaries. Within the New York Special Agent in Charge office, the Homeland Security Investigations Airport Group is responsible for the identification, disruption, and dismantlement of transnational criminal organizations attempting to exploit vulnerabilities within the air transportation system at JFK. The Homeland Security Investigations Airport Group's areas of concern at JFK include:Contraband smuggling,

- Currency smuggling,
- National security,
- Human smuggling/trafficking,
- Sexual tourism,
- Insider threat, and
- Theft and trafficking of cultural heritage and art.

The JFK Office of Professional Responsibility investigates criminal and administrative misconduct committed by ICE and CBP employees and contractors. This office also addresses complaints of people pretending to be ICE and CBP employees or attempted bribery.

We audited IT security controls at the following ICE locations:

- The Special Agent in Charge New York Office, located in Building No. 75,
- Office of Professional Responsibility, located in Building No. 75, and
- Joint Narcotics and Smuggling Unit, located in JFK Terminal 4.

ICE staff at these locations use the following systems:

- Office File and Print Servers – provide workstation, laptop, print services, and file capability to all ICE employees. File servers provide a networked file repository and print servers allow networked printing.

- ICE Communication over Networks – provides support for all network devices and data communications used by ICE and at 287(g) sites.7

- A communication surveillance and analysis system that helps Homeland Security Investigations staff to gather intelligence and collect live data in support of ICE's law enforcement mission. Specifically, the system assembles historical telephone records, monitors telephone and Internet communications, and permits searches of warrant data from online providers. The communication surveillance and analysis system connects to the ICE network infrastructure or on a separate standalone network. This is not a designated mission essential system.

U.S. Secret Service

USSS have nine agents and two administrative personnel located at JFK that report directly to the USSS New York Field Office in Brooklyn, NY. This office is the only USSS office located at an airport.

The agents assigned to the office handle between 750 and 800 arrivals and departures of USSS protected individuals/groups, including Prime Ministers and current and former U.S. Presidents and immediate family members, at JFK and LaGuardia Airports. Each September, the United Nations General Assembly in New York City impacts the JFK Resident Office with over 300 arrivals and departures at JFK and LaGuardia Airports and an additional 42 temporarily assigned agents/officers.

The office also works closely with CBP to seize counterfeit United States currency entering JFK Airport at the passenger and cargo terminals. Since May 2010, DHS seized United States currency totaling over $4 million. The employees of the USSS office use Windows 7, Office 2010, and web—based applications. The service's New York Field Office Technical Operations Squad performs all IT updates, equipment repairs, and installation of new equipment.

[7] The 287(g) program, under the *Immigration and Nationality Act*, as amended, allows a state and local law enforcement entity to receive delegated authority for immigration enforcement within its jurisdiction.

Appendix D
Major Contributors to This Report

Sharon Huiswoud, IT Audit Director
Sharell Grady, IT Audit Manager
Beverly Dale, IT Senior Auditor
Robert Durst, Senior Program Analyst
Frederick Shappee, Senior Program Analyst
Daniel McGrath, Referencer

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
DHS CISO
DHS CISO Audit Liaison
CBP CIO
CBP Audit Liaison
ICE CIO
ICE Audit Liaison
TSA CIO
TSA Audit Liaison
USSS CIO
USSS Audit Liaison
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

Image not available for this document, ID: 0.7.747.6384-000003

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

3 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

Audit Liaison Division

Integrity | Partnership | Support

Attachment A

OFFICE OF INSPECTOR GENERAL

Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport (Redacted) (Revised)

Homeland Security

January 16, 2015

OIG-15-18 (Revised)

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

January 16, 2015

MEMORANDUM FOR: The Honorable Chip Fulghum
Acting Under Secretary for Management

FROM: John Roth John Roth
Inspector General

SUBJECT: *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport*

Attached for your information is our revised final report, *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport.* This report contains findings and recommendations for improving security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS information technology infrastructure at this airport.

The procedural history of this report elicits an unfortunate commentary on the manner in which the Department handled this matter and bears review:

- We provided a draft of this report on July 22, 2014 to the Chief Information Officer for review. Pursuant to *Department of Homeland Security Directive 077-01, Follow-up, and Resolution for Office of Inspector General Report Recommendations,* we asked for agency comments, including a sensitivity review, within 30 days of receipt of the draft. This would have made the report due on or about August 22, 2014. Almost a week later, on August 27, 2014, the DHS Chief of Staff requested an extension to provide a response and technical comments. I granted the extension until September 17, 2014.

- On October 20, 2014, nearly 60 days after the original due date for agency comments, the Departmental GAO-OIG Liaison Office finally conveyed to us TSA's response to our request for a sensitivity review by marking several passages in the report as SSI. I disagree with this determination.

- On November 19, 2014, I sent a formal challenge memo to TSA Administrator John Pistole expressing my disagreement. Administrator Pistole had authority over all TSA programs and operations, including oversight of the SSI programs, and is my counterpart in DHS' leadership.

- Having received no reply, on December 16, 2014, I wrote to Administrator Pistole a second time, noting that this report had languished as a result of TSA's sensitivity review, and again requesting that he remove the SSI deletions from the report. As with the November 19, 2014 letter, I received no reply.

- Finally, on January 13, 2015, over five months after submitting the report for sensitivity review, and two months after writing to Administrator Pistole, I received a decision, not from the Acting TSA Administrator, but from the head of the SSI program office – the very same office that initially and improperly marked the information as SSI. Not surprisingly, the office affirmed its original redaction to the report.

I am disappointed in both the substance of the decision as well as its lack of timeliness. In 2006, Congress, concerned about delays in appeals of this nature, directed the Department to revise DHS Management Directive 11056.1 to require TSA to require timely SSI reviews. Given the clear requirement for timely SSI reviews in response to requests from the *public*, we hoped that TSA would approach an SSI appeal from the *Inspector General* with similar diligence, especially because TSA was aware of our deadlines.

Now, to meet our reporting requirement, we are compelled to publish a redacted report with SSI markings and will again ask the head of TSA to overrule the SSI program office's decision.

I believe that this report should be released in its entirety in the public domain. I challenged TSA's determination because this type of information has been disclosed in other reports without objection from TSA, and because the language marked SSI reveals generic, non-specific vulnerabilities that are common to virtually all systems and would not be detrimental to transportation security. My auditors, who are experts in computer security, have assured me that the redacted information would not compromise transportation security. Our ability to issue reports that are transparent, without unduly restricting information, is key to accomplishing our mission. Congress, when it passed the *Reducing Over-Classification Act* in 2010, found that over-classification "interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information."

Consistent with our responsibilities under the *Inspector General Act*, and in compliance with 49 CFR 1520, we will provide appropriately marked and unredacted copies of our report to appropriate Congressional committees with oversight and appropriation responsibility for the Department of Homeland Security. We will post a redacted version of the report on our website pending a decision from the Acting TSA Administrator.

I appreciate your attention to this matter. Should you have any questions, please call me, or your staff may contact Sondra McCauley, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4041.

Attachments

cc: Melvin Carraway, Acting Administrator
Transportation Security Administration

The Honorable R. Gil Kerlikowske
Commissioner, U.S. Customs and Border Protection

The Honorable Sarah Saldaña
Assistant Secretary, U.S. Immigration and Customs Enforcement

Joseph Clancy, Acting Director
United States Secret Service

Attachment 1

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

NOV 1 9 2014

MEMORANDUM FOR: The Honorable John Pistole
Administrator
Transportation Security Administration

FROM: John Roth John Roth
Inspector General

SUBJECT: Office of Inspector General's Challenge to Sensitive Security Information Office's Request to Mark OIG report: *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport* as SSI
OIG *Project No: 14-082-ITA-DHS*

The Inspector General Act requires the Office of Inspector General (OIG) to conduct audits and investigations that promote the economy, efficiency, and effectiveness of DHS programs and operations, and to inform the Secretary, Congress, and the public about any problems and deficiencies we identify. Our ability to issue reports to the public that are transparent, without unduly restricting information, is key to accomplishing our mission.

I am concerned that the Department's review and response to our draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport*, indicated that several statements within the report were determined to be Sensitive Security Information (SSI). I disagree with this determination and I am submitting this formal challenge according to procedures outlined in DHS Management Directive MD 11056.1, Sensitive Security Information. Under DHS MD 11056.1.F.2, a formal challenge may be submitted, in writing, to the person who made the SSI markings or to the SSI Office.

We issued the draft report, *Technical Security Evaluation of DHS Activities at JFK International Airport,* to the Department on July 22, 2014. On August 6, 2014, a SSI Senior Program Analyst, provided a response and marked as SSI several passages in this report. See Attachment A for a copy of this draft report with the suggested SSI content highlighted. I recognize the SSI Office's process to identify and safeguard SSI information. However, I believe the information in our draft report was

improperly marked as SSI and I am challenging this determination based on the following:

First, the same or similar information as that marked SSI in the current draft report was disclosed to the public in previously released DHS OIG and GAO reports. The Department reviewed and approved the content of these previously released reports and did not determine at that time that the information was SSI. For example:

- On page 5 of our draft report, we discuss physical security issues in TSA's space at JFK airport. The SSI Office marked this information as SSI based on 49 C.F.R. § 1520.5(b) (5). I challenge this request. In GAO audit report *General Aviation: Security Assessments at Selected Airports*, GAO-11-298 dated May 2011, GAO published similar information. Specifically, the GAO report discusses and reports the security measures and potential vulnerabilities at selected airports. (page 7, Attachment B)
- Also, on page 5 of our draft report, we display a picture of TSA equipment in a corridor accessible by unsecured double doors to public area prior to TSA terminal security checkpoint. The SSI Office marked this picture SSI. I challenge this request. This is a picture of IT equipment similar to the IT equipment pictured in figures 4, 5, and 6 of our draft report, yet the SSI Office did not mark those figures SSI. This item shows an example of a TSA equipment cabinet that is in an area accessible to non TSA staff and the public. This risk can be controlled and eliminated by TSA simply securing the terminal corridor from unauthorized access. In addition, our report did not provide the specific location of this cabinet.
- On pages 14 and 21 of our draft report, the SSI office marked one sentence on each page as SSI information. These sentences are located in the TSA (page 14) and CBP (page 21) Patch Management Sections of our report. I challenge this request. Similar or the same wording was used in our last two publically released technical security airport reviews at Dallas Ft. Worth (*Audit of Security Controls for DHS Information Technology Systems at Dallas/Ft. Worth International Airport*, OIG-14-132) and Atlanta's Hartsfield (*Technical Security Evaluation of DHS Activities at Hartsfield Jackson Atlanta International Airport*, OIG-13-104) airports. (pages 10, 18, and 25 in Attachment C and pages 10, 20, and 31 in Attachment D)

- Also on pages 14 and 21 of our draft report, the SSI office marked information in the tables in the TSA and CBP Patch Management sections of the report as SSI information. I challenge this request. Similar content in the same table format was reported in our last two publically released DHS OIG audit reports on Dallas/Ft. Worth, OIG-14-132, and Atlanta Hartsfield airports OIG-13-104. (pages 10, 18, and 25 in Attachment C and pages 10, 20, and 31 in Attachment D)

Second, although the SSI Office marked information in the TSA and CBP Patch Management sections of the draft report as SSI, the SSI Office did not mark the same information in the ICE section of the same report as SSI. Specifically, the ICE section of the draft report includes the same table and wording regarding scanning vulnerabilities that is in the TSA and CBP sections. However, the SSI office did not mark the ICE information as SSI. The SSI determination appears to be inconsistently applied.

Further, even if past reports had not released similar information, I still do not believe its release in this report would be detrimental to transportation security. For example, the language marked SSI reveals generic vulnerabilities that are common to virtually all systems. In addition, the descriptions of the vulnerabilities are not specific enough to be detrimental.

For these reasons, I am requesting that you reconsider and remove your SSI markings from our draft report. These markings impede the effectiveness and transparency of our office. I feel that based on the reasons I have outlined above, our OIG report, *Technical Security Evaluation of DHS Activities at JFK International Airport,* should be released in its entirety in the public Domain.

I appreciate your attention to this matter. Please feel free to contact me with any questions.

cc: Jim Crumpacker, Director, DHS GAO/OIG Liaison Office
Shelly Peterson, Audit Liaison for the Chief Information Officer
Susan Perkins, TSA, Audit Liaison
Tamara Lilly, DHS CISO, Audit Liaison
John Buckley, CBP, CISO
Judy Wright, CBP, Audit Liaison
Tom DeBiase, ICE, Acting CISO

Joanna Perkins, ICE, Audit Liaison
Jill Vaughan, TSA, CISO
Thomas Feltrin, TSA, Audit Liaison
Doug Blair, SSI Program Chief
Rob Metzler, Senior Analyst

Attachment 2

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

DEC 1 6 2014

MEMORANDUM FOR: The Honorable John Pistole
Administrator
Transportation Security Administration

FROM: John Roth John Roth
Inspector General

SUBJECT: Follow up to my Challenge Memo to the SSI Markings to draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport-Sensitive Security Information*

I am writing to follow up on the memo I sent you on November 19, 2014, regarding my challenge to Sensitive Security Information (SSI) markings to our draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport.* We are preparing to issue this report as final. However, I am concerned that I have not heard back from you regarding my request to remove the SSI markings from our report so that we may issue it in its entirety in the public domain.

In response to a law passed by the Congress in 2006, the Department revised DHS Management Directive (MD) 11056.1, to require TSA to ensure a timely SSI review of public requests for release of information. Given MD 11056.1, section V.B.7's requirement for timely SSI reviews in response to requests from the public, we hoped that TSA would approach our SSI appeal from a fellow component with similar diligence, especially since TSA is aware of our deadlines. We are disappointed.

In its October 20, 2014, response to our draft report, the Department indicated that several statements within the report were determined to be SSI. I disagree with the markings and submitted my challenge to you in accordance with guidance provided under MD 11056.1.

I again request that you reconsider and remove the SSI markings from our draft report. I recognize the SSI Office's process to identify and safeguard SSI information. However, I believe that improperly marking information in our draft report as SSI impedes our ability to issue reports to the public that are transparent, without unduly restricting information, which is key to accomplishing our mission. Per DHS MD

11056.1, VI.A.3, SSI markings should not be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency.

This report has languished for months because of TSA's sensitivity review. Absent a decision from you, we will be forced to publish a redacted report to meet our timeliness requirements. The report will contain our objections to the redactions. Consistent with our responsibilities under the *Inspector General Act*, we will provide unredacted copies of our report to Congressional Committees with oversight and appropriations responsibility for the Department of Homeland Security.

I appreciate your personal attention to this matter and I await your response. Should you have any questions, please call me.

Attachment

Errata page for OIG-15-18

Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport (Redacted)

Changes made for Redactions page 5, 1st paragraph and figure 2 (see below):

Revised SSI marking redactions applied.

Change made to the Management Comments and OIG Analysis section, page 31, 1st paragraph (see below):

The following statement has been removed from our report for clarity:

We consider these recommendations resolved, but open pending verification of corrective and planned actions and supportive documentation.

Change made to the Management Comments and OIG Analysis section, page 39, 1st paragraph (see below):

The following statement has been removed from our report for clarity:

We consider these recommendations resolved, but open pending verification of corrective and planned actions and supportive documentation.

The revisions did not change the findings or recommendations made in this report.

Table of Contents

Executive Summary 1

Background 2

Results of Audit 4

TSA Did Not Comply Fully with DHS Sensitive Systems Policies 4
Recommendations 16
Management Comments and OIG Analysis 17

CBP Did Not Comply Fully with DHS Sensitive Systems Policies 20
Recommendations 26
Management Comments and OIG Analysis 27

ICE Did Not Comply Fully with DHS Sensitive Systems Policies 29
Recommendations 33
Management Comments and OIG Analysis 34

USSS Fully Complied with DHS Sensitive Systems Policies 36

Department's Noncurrence 36

Appendixes

Appendix A: Objectives, Scope, and Methodology 37
Appendix B: Management Comments to the Draft Report 39
Appendix C: DHS Activities at JFK Airport 44
Appendix D: Major Contributors to This Report 49
Appendix E: Report Distribution 50

Abbreviations

Airport Authority	Port Authority of New York and New Jersey
CBP	U.S. Customs and Border Protection
CCTV	closed-circuit television
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security

FAMS	Federal Air Marshall Service
FAMSNet	Federal Air Marshall Service Network
GAO	Government Accountablity Office
ICE	U.S. Immigration and Customs Enforcement
IT	information technology
JFK	John F. Kennedy International Airport
OIG	Office of Inspector General
OMB	Office of Management and Budget
OneNet	DHS One Network
PIA	privacy impact assessment
PII	personally identifiable information
PTA	privacy threshold assessment
Security System	Airport Authority Selected Surveillance Systems
TECS	Treasury Enforcement Communication System
TSA	Transportation Security Administration
TSANet	Transportation Security Administration Network
UPS	uninterruptible power supply
USSS	United States Secret Service

Executive Summary

As part of our Technical Security Evaluation Program, we evaluated technical and information security policies and procedures of Department of Homeland Security components at the John F. Kennedy International Airport. Four Department components – the Transportation Security Administration, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Secret Service – operate information technology systems that support homeland security operations at this major airport.

Our evaluation focused on how these components have implemented operational, technical, and management controls for computer security at the airport and nearby locations. We performed onsite inspections of the areas where these assets were located, interviewed departmental staff, and conducted technical tests of computer security controls. We also reviewed applicable policies, procedures, and other relevant documentation.

The Department's sensitive system security policies, the information technology security controls implemented at several sites had deficiencies that, if exploited, could have resulted in the loss of confidentiality, integrity, and availability of the components' information technology systems. We identified numerous deficiencies in the information technology security controls associated with the Transportation Security Administration. Additionally, operational environmental controls and security documentation needed improvement. Further, information security vulnerabilities were not resolved timely. Technical security controls for Customs and Border Protection and Immigration and Customs Enforcement information technology resources also needed improvement. The Transportation Security Administration, Customs and Border Protection, and Immigration and Customs Enforcement did not perform required security authorization or privacy reviews on closed–circuit television and surveillance monitoring room technology. The U.S. Secret Service fully complied with DHS sensitive security policies at the airport.

The draft report included 14 recommendations and DHS concurred with 13 of the 14 recommendations. DHS did not concur with recommendation number six. We do not agree with DHS's response to this recommendation, as it does not provide for corrective actions to address the security and privacy concerns identified in our report. To help ensure that these security and privacy concerns get addressed properly, we issued two additional recommendations for the DHS Chief Information Officer and DHS Chief Privacy Officer. We have included a copy of the Department's comments to the draft report in their entirety in appendix B.

Background

We designed our Technical Security Evaluation Program to provide senior Department of Homeland Security officials with timely information on whether they had properly implemented DHS information technology (IT) security policies at critical sites. Our program audit was based on the requirements identified within *DHS Sensitive Systems Policy Directive 4300A,* version 10.0, which provides direction to DHS component managers and senior executives regarding the management and protection of sensitive systems. This directive and an associated handbook outline policies on the operational, technical, and management controls necessary to ensure confidentiality, integrity, and availability within the DHS IT infrastructure and operations. These controls are as follows:

- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people to improve system security. For example, operational control mechanisms include physical access controls that restrict the entry and exit of personnel from an area, such as an office building, data center, or room, where sensitive information is accessed, stored, or processed.

- **Technical Controls** – Focus on security controls executed by information systems. These controls provide automated protection from unauthorized access; facilitate detection of security violations; and support applications and data security requirements. For example, technical controls include passwords for systems.

- **Management Controls** – Focus on managing both the system information security controls and system risk. These controls include risk assessments, rules of behavior, and ensuring that security is an integral part of both system development and IT procurement processes.

We evaluated security controls for IT systems that support homeland security operations of the Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Secret Service (USSS) at John F. Kennedy International Airport (JFK). Figure 1 shows Terminal Four at JFK.

Figure 1-JFK Terminal Four

JFK is the sixth busiest airport in the United States. With arrivals and departures from almost every international airline in the world, JFK is an international gateway for passengers and heavy freight. Below are some facts about JFK.

- JFK, on the Jamaica Bay in New York City, is a designated port of entry.[1] The airport covers over 4,930 acres, including 30 miles of roadway. JFK has 6 operating airline terminals and more than 125 airline gates.

- Port Authority of New York and New Jersey (Airport Authority) operates JFK under a lease with the City of New York since 1947, with the current lease continuing until 2050. The Airport Authority has invested over $10 billion in the airport.

- JFK contributes about $30.6 billion in economic activity annually to the New York/New Jersey region, generating approximately $4.2 billion in direct wages; 71,000 jobs and indirect wages of $30.5 billion for 213,400 jobs.

- JFK is a leading international air cargo center. This facility has more than four million square feet of office and warehouse space dedicated to cargo operations serving the New York and New Jersey region. The entire air cargo area has automated and computer-controlled terminals containing one or more restricted access sites.

[1] Port of entry is defined as a designated controlled entry points into the United States from foreign countries.

See appendix C for specific details of DHS component activities at the JFK airport.

Results of Audit

TSA Did Not Comply Fully with DHS Sensitive Systems Policies

TSA did not comply fully with DHS operational, technical, and management policies for its servers and switches operating at JFK. Specifically, physical security and access controls for numerous TSA server rooms and communication closets were deficient. Additionally, TSA had not implemented known software patches to its servers at JFK. Finally, TSA did not designate the closed-circuit television (CCTV) cameras as a DHS IT system nor did it implement the applicable, operational, technical, and managerial controls for the cameras. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability, of the data stored, transmitted, and processed by TSA at JFK.

Operational Controls

We evaluated TSA server rooms and communication closets containing IT assets at JFK. We identified operational controls that did not conform fully to DHS policies. Specifically, we identified deficiencies in physical security, visitor logs, the fire protection system, storage and housekeeping, electronic power supply protection, and humidity and temperature controls.

Physical Security

Adequate access controls have not been established limiting access to TSA sensitive equipment in JFK terminals. For example, [redacted] located [redacted] contained DHS locked equipment cabinets located [redacted] with non-DHS IT equipment. According to TSA staff, technical representatives did not know the total number of non-DHS personnel that had access to [redacted] In addition, [redacted] contained unsecured TSA equipment and were accessible to non-DHS individuals. Specifically, as shown in figure 2, a TSA [redacted] cabinet was located [redacted] airport. The doors between the two areas did not lock, and airport employees walked through the area. [redacted]

[redacted]

The door to the secure Explosive Detection Systems room, where TSA reviews x-ray images of luggage to determine if suspicious checked luggage requires additional inspection, was propped open to vent a portable air conditioning unit, violating physical security controls. Figures 3a, 3b, and 3c show the required access control into the room, a secondary door to the room left open, and an air conditioning unit venting hot air out through the open door.

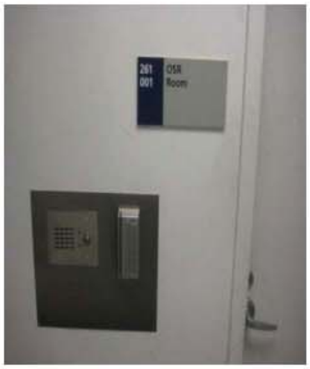


Figure 3a-Access Control

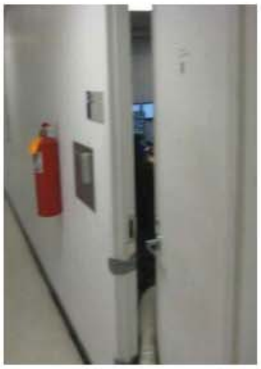


Figure 3b-Unsecured Door

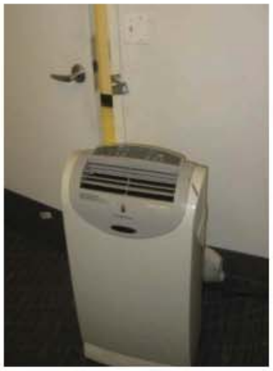


Figure 3c-Climate Control

According to DHS Sensitive System Policy Directive 4300A:

> Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.

Physical security vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of TSA data. Unauthorized access to TSA server rooms may result in the loss of IT processing capability used for passenger and baggage screening.

Visitor Logs

At JFK, TSA did not have visitor logs in any of its communication rooms to document the entry and exit of visitors to these rooms that contain sensitive IT equipment.

According to DHS Sensitive System Policy Directive 4300A:

> Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data. They shall be escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.

When unauthorized individuals gain access to locations where sensitive computing resources reside, there is an increased risk of system compromise and data confidentiality, integrity, and availability concerns.

Fire Protection System

Fire protection, detection, and suppression controls were not present in many TSA communication rooms. Specifically, 14 of the 21 rooms inspected that contained sensitive equipment did not have fire extinguishers. Additionally, 8 of the 21 rooms did not have a fire suppression system installed. As a result, 5 rooms were in violation of fire protection policy. Table 1 shows the existence or lack of fire protection equipment at the locations inspected.

Table 1-TSA Fire Protection

TSA Fire Protection			
Identification of the room	**Smoke Detector**	**Fire Extinguisher**	**Fire Suppression**
TSA Location 1	Yes	No	Yes
TSA Location 2	Yes	No	Yes
TSA Location 3, TSA/FAMS	No	No	Yes
TSA Location 4, Terminal 1	No	No	No
TSA Location 5, Terminal 1	No	No	Yes
TSA Location 6 Terminal 1	Yes	No	Yes
TSA Location 7, Terminal 2	No	No	Yes
TSA Location 8, Terminal 4	No	No	Yes
TSA Location 9, Terminal 4	Yes	Yes	No
TSA Location 10, Terminal 4	No	No	No
TSA Location 11, Terminal 4	Yes	Yes	No
TSA Location 12, Terminal 5	No	No	Yes
TSA Location 13, Terminal 5	Yes	No	Yes
TSA Location 14, Terminal 5	No	Yes	Yes
TSA Location 15, Terminal 7	No	No	No
TSA Location 16, Terminal 7	No	Yes	No
TSA Location 17, Terminal 7	No	No	No
TSA Location 18, Terminal 7	No	No	No
TSA Location 19, Terminal 8	Yes	Yes	Yes
TSA Location 20, Terminal 8	No	Yes	Yes
TSA Location 21, Terminal 8	No	Yes	Yes

According to DHS 4300A Sensitive Systems Handbook:

> Fire protection systems should be serviced by professionals on a recurring basis to ensure that the systems stay in proper working order. The following should be considered when developing a fire protection strategy:
>
> - When a centralized fire suppression system is not available, fire extinguishers should be readily available.
> - Facilities should make available/provide Class C fire extinguishers, designed for use with electrical fire and other types of fire.
> - Fire extinguishers should be located in such a way that a user would not need to travel more than 50 feet to retrieve one.

Compounding the issue of fire detection and mitigation, only 7 of 21 the rooms inspected contained smoke detectors. Smoke detectors alert the appropriate personnel of a potential fire and possible hazard.

The DHS 4300A Sensitive Systems Handbook also states:

> In addition to the physical security controls discussed above, facility managers and security administrators must also ensure that environmental controls are established, documented, and implemented to provide needed protection in the following areas:
>
> - Fire protection, detection, and suppression

In addition to DHS 4300A Sensitive Systems Handbook, TSA's Information Assurance Handbook states:

> The Facility Security manager shall employ and maintain fire suppression and detection devices/systems (to include sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors) for the TSA facility information systems that are supported by an independent energy source. When centralized fire suppression is not available, Class C fire extinguishers should be readily available. Each class C fire extinguisher

should be located in such a way that the user would not need to travel more than 50 feet to retrieve it.

The lack of fire notification capabilities and unmitigated suppression system vulnerabilities place at risk the availability of TSA data. For example, sensitive equipment damaged by fire may not be available for TSA's passenger and baggage screening processes.

Storage and Housekeeping

Several TSA communication closets located in the JFK terminals contained storage items and cleaning supplies. For example, we found TSA equipment on top of an unlocked TSA telecommunication cabinet surrounded by a ladder, boxes, trash, and cleaning supplies. The ladder, boxes, and cleaning supplies are all harmful to IT equipment. Additionally, there was no sign in sheet, and non-TSA personnel used the room for equipment storage. Figures 4 and 5, show cleaning supplies and maintenance equipment stored with TSA IT hardware in a communication room and communication closet.

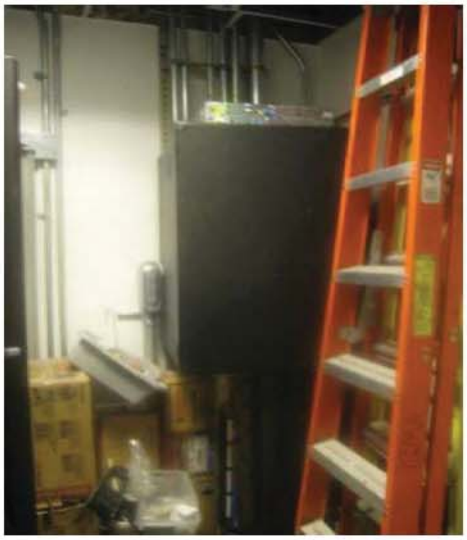


**Figure 4 -
Unlocked Communication Cabinet with Unsecured TSA Equipment**

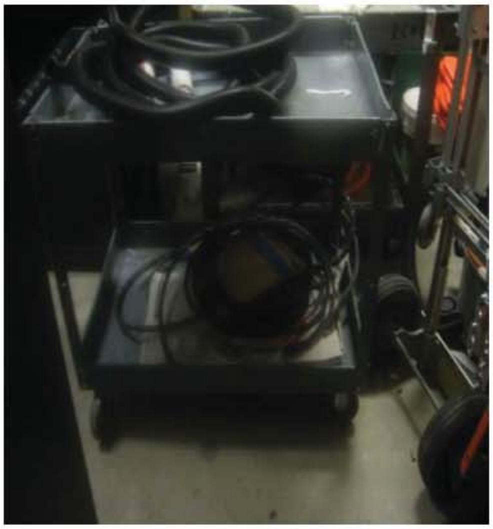


**Figure 5 -
Communication Room used as Storage**

Items being stored in the room were an obstruction and preventing access to the TSA IT equipment cabinets. A lack of housekeeping and maintenance caused a buildup of dust on TSA IT hardware stored within cabinets as shown in figure 6.

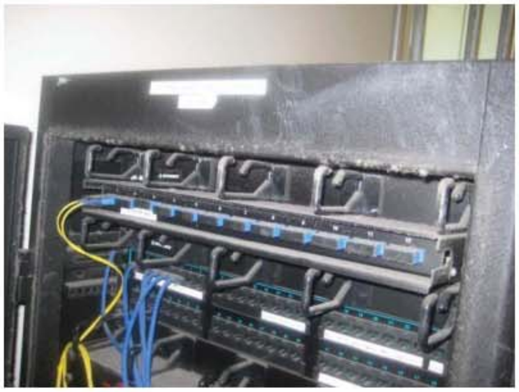


Figure 6- Dust covered Sensitive Equipment

According to DHS 4300A Sensitive Systems Handbook:

- Dusting of hardware and vacuuming of work area should be performed weekly with trash removal performed daily. Dust accumulation inside of monitors and computers is a hazard that can damage computer hardware.
- Cleaning supplies should not be stored inside the computer room.

Storage and housekeeping issues place the availability of TSA data at risk. Computer hardware damaged by dust and debris has the potential to cause delays for TSA's passenger and baggage screening processes.

Electronic Power Supply Protection

TSA did not have an operable uninterruptible power supply (UPS) in three communication cabinets. Figure 7 shows an unlocked cabinet and figure 8 shows inoperable UPS equipment.

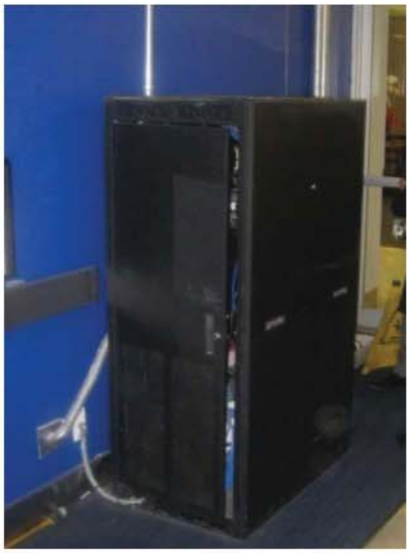


Figure 7-
Accessible Equipment

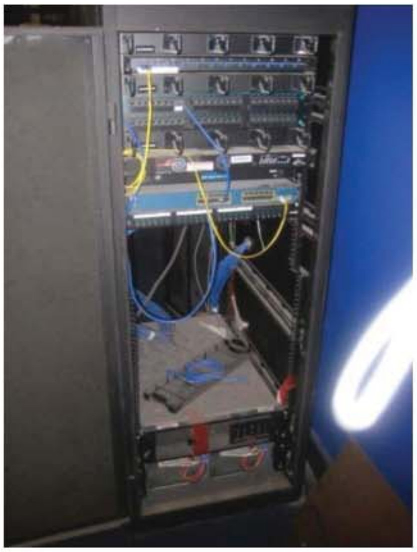


Figure 8-
Inoperable UPS

A sensitive equipment cabinet located in a public area was unlocked and left open to run an extension cord to a nearby electrical outlet for power. Upon closer inspection, we determined that the UPS was inoperable and not being used to provide backup power to IT equipment. Additionally, the attached extension cord prohibited the cabinet from closing and locking.

According to the *DHS 4300A Sensitive Systems Handbook*:

> Electrical power must be filtered through an UPS system for all servers and critical workstations and surge suppressing power strips used to protect all other computer equipment from power surges.

Electrical power supply vulnerabilities place TSA data availability at risk. For example, TSA servers that are not connected to a working UPS may not operate following a power outage.

Humidity and Temperature Controls

TSA did not have any device to measure humidity in the 21 server/switch rooms that we visited at JFK. Additionally, 13 out of the 21 server/switch rooms did not contain temperature sensors. Of the eight rooms that had temperature sensors, only two had temperature readings within the acceptable range established by DHS policy.

According to the *DHS 4300A Sensitive Systems Handbook*:

- Humidity should be at a level between 35 percent and 65 percent.
- Temperatures in computer storage areas should be between 60 and 70 degrees Fahrenheit.

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Technical Controls

TSA's implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, identified vulnerabilities on TSA servers at JFK had not been resolved or patched in a timely fashion.

Patch Management

In February 2014, we observed TSA staff scan two servers located at JFK for vulnerabilities. [redacted][2] Table 2 provides the number of vulnerabilities by server.

[2] Critical vulnerabilities should be addressed immediately due to the imminent threat to a network.

Table 2- Critical, High, and Medium Vulnerabilities

TSA Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]

According to *DHS Sensitive Systems Policy Directive 4300A*:

> Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.

Server vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of TSA data.

Management Controls

TSA's implementation of management controls for the Airport Authority's Security Systems operating at JFK did not conform fully to DHS policies. Specifically, TSA had not designated the Security System as a DHS IT system. As a result, TSA had not performed the applicable security authorization processes and privacy requirements over the surveillance system at JFK terminals.

CCTVs and Surveillance Systems

TSA did not designate the JFK CCTV cameras and surveillance system as DHS IT systems. As a result, the component did not implement the applicable, operational, technical, and managerial controls for the cameras and the systems. TSA officials stated that it was not responsible for the cameras and surveillance system because they belong to the Airport Authority.

However, TSA provided the funding for the JFK CCTV cameras and surveillance systems to the New York Airport Authority. The funding was an estimated $7.2 million to design, install, and maintain the JFK CCTV intrusion detection systems and other surveillance equipment. The Airport Authority Selected Surveillance Systems (Security System) includes CCTV cameras, detection systems, other surveillance hardware, storage equipment, and associated electrical cabling, and

support facilities monitored at JFK. The Airport Authority sets the conditions for shared use of these systems throughout JFK. Figure 9 shows the TSA's Security System.

Figure 9-Security System at JFK

According to the agreement between the Airport Authority and TSA, the Security System provides greater surveillance of TSA areas to enhance security at JFK and assists in resolution of law enforcement issues. The Airport Authority is the owner of the Security System and is responsible for the repairs and maintenance. All media generated from the Security System remains with the Airport Authority. Although, the Airport Authority owns the systems, TSA controls the system design, identification of milestones, and who has allowable access to the system data. TSA officials also have unlimited ability to access information from the Security System to conduct TSA administrative or Top Secret criminal investigations.

The Security System collects images from all cameras to a video management system that stores the information for a minimum of 31 days. Since information that DHS uses is being stored, transmitted, and monitored on this system, and the Port Authority is operating this system on behalf of TSA, then TSA has the requirement to designate the Security System as a DHS IT system. However, TSA officials stated that because this system belongs to the Airport Authority it did

not need to conduct required security authorization processes, a privacy threshold analysis (PTA), or a privacy impact assessment (PIA).[3]

According to *DHS Sensitive Systems Policy Directive 4300A*:

> A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf.

DHS Sensitive Systems Policy Directive 4300A states that Component Chief Information Security Officers (CISO) shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

[3] A privacy threshold analysis is performed to determine if additional privacy compliance documentation is required, such as a privacy impact assessment. A privacy impact assessment is a publicly released assessment of the privacy impact of an information system and includes an analysis of the personally identified information collected, stored, and shared.

PII includes photographic facial images and any other unique identifying number or characteristic.

Also, Office of Management and Budget (OMB) M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when it uses IT to collect new information.

TSA has not fulfilled security authorization or privacy requirements for the cameras and surveillance systems at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put this information at risk, and lead to violations of U.S. privacy laws and DHS policy.

Recommendations

We recommend that the TSA Chief Information Officer (CIO):

Recommendation #1:

Comply with DHS policy concerning physical security, housekeeping and electronic power supply protection at all locations at JFK that contain TSA IT assets.

Recommendation #2:

Comply with DHS policy concerning fire protection at all locations at JFK that contain TSA IT assets.

Recommendation # 3:

Maintain JFK servers and network rooms free of excess storage that may cause damage to the equipment.

Recommendation #4:

Obtain humidity and temperature sensors for the JFK server rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Recommendation #5:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #6:

Designate the intrusion detection and surveillance Security Systems as DHS IT systems and implement applicable management, technical, operational, and privacy controls and reviews.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Assistant Director, Departmental Government Accountability Office (GAO) OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #1 through #5, but non-concurred with recommendation #6. Additionally, TSA has already taken actions and has submitted supporting documentation to resolve the reported deficiencies for recommendations #1, #3, and #5. We consider these recommendations resolved, but open pending verification of corrective and planned actions and supportive documentation.

Recommendation #1:

DHS concurred with recommendation 1. TSA officials recognize the need to comply with DHS policies on physical security, housekeeping, and electrical power supply protection by conducting quarterly cleaning of all IT equipment cabinets as well as ensuring that all uninterrupted power supplies are operational. TSA took several corrective actions and submitted supporting documentation. We agree that the steps TSA is taking, and plans to take, will satisfy this recommendation. Our recommendation will remain open and resolved until we receive and review supporting documentation for the corrective actions.

Recommendation #2:

DHS concurred with recommendation 2. TSA officals recognize the need to comply with the DHS policy concerning fire protection. TSA plans to take corrective actions to ensure that all locations at JFK that contain TSA IT assets are equipped with fire extinguishers. Additionally, TSA plans to verify the presence of other required fire protection equipment at all of its locations at JFK. TSA estimated that corrective actions would be completed by November 30, 2014.

We agree that the steps that TSA is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until we receive and review the corrective actions and supporting documentation.

Recommendation #3:

DHS concurred with recommendation 3. TSA's response outlines corrective actions for the removal of the excess items and the assurance to refrain from using IT equipment rooms as storage areas. We agree that the steps TSA is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until we receive and review the corrective actions and supporting documentation.

Recommendation #4:

DHS concurred with recommendation 4. TSA recognizes that temperature and humidity levels in computer storage areas should be between 60 and 70 degrees Fahrenheit and at a level between 35 percent and 65 percent, respectively. TSA plans to coordinate with facilities management to ensure that the Airport Authority complies with these requirements. TSA estimated that the corrective actions would be completed by October 31, 2014. We recognize these actions as positive steps and look forward to learning more about the continued progress in the future. This recommendation will remain open and resolved pending receipt and verification of planned actions and supporting documentation

Recommendation #5:

DHS concurred with recommendation 5. TSA stated that it remediated the identified vulnerabilities. TSA also stated that another subsequent security scan of the JFK servers was conducted to ensure vulnerabilities identified previously were no longer present on the servers. TSA provided supporting documentation for this recommendation. This recommendation will remain open and resolved pending verification of corrective actions and supporting documentation.

Recommendation #6:

DHS did not concur with recommendation 6. Instead of addressing directly our recommendation to designate detection and surveillance systems as DHS IT systems and to initiate appropriate IT security and privacy controls, TSA indicated it does not have a relationship at the JFK Airport that meets the definition of DHS 4300A Sensitive Systems Handbook for DHS IT systems. In TSA's

response, it stated that, because the intrusion detection and surveillance security systems are owned and operated by the Airport Authority, it had no responsibility to ensure that IT security and privacy controls were met.

According to the DHS Sensitive Systems Policy Directive 4300A, however, a DHS IT system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf. The systems at JFK transmit, store, and process data on behalf of DHS. Based on the Department's definition, these systems are IT systems and need to be treated as such by DHS. Because TSA has refused to define the detection and surveillance systems as DHS IT systems, TSA did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

We do not agree with DHS's response to this recommendation. The response does not provide for corrective actions to address the security and privacy concerns identified. DHS needs to perform security and privacy reviews of the surveillance systems at JFK airport. By not peforming these reviews, vulnerabilitilies may exist that may put the information collected at risk and lead to security breaches, and violations of DHS policy, and U.S. privacy laws. To assist in this process, we have added additional recommendations, #15 and #16, to our report that will need to be addressed before we can resolve the status of this recommendation.

We look forward to reviewing TSA's progress in the future. However, this recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

CBP Did Not Comply Fully with DHS Sensitive Systems Policies

CBP did not comply fully with DHS operational, technical, and management controls. Specifically, several CBP servers and telecommunication rooms did not contain humidity and temperatures sensors. Additionally, the temperature of several of the rooms reviewed with sensors had room temperatures that exceeded temperature ranges established by DHS policy. The humidity control readings for these rooms were within the ranges set by DHS policy. Also, CBP had an unlocked and open switch device in an open storage area allowing the potential for unauthorized access. In addition, CBP had not implemented known information security software patches to its servers at JFK. Finally, CBP did not designate the CCTV cameras and surveillance room as DHS IT systems nor did they implement the applicable, operational, technical, and managerial controls for these JFK systems. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by CBP at JFK.

Operational Controls

CBP server rooms and communication closets at JFK were clean and well maintained. However, onsite implementation of operational controls did not conform fully to DHS policies. For example, temperatures in CBP JFK server rooms were not within the temperature range recommended by the DHS 4300A Sensitive Systems Handbook. Additionally, one of the CBP sites did not have adequate equipment to prevent unauthorized access to CBP communication switches.

Humidity and Temperature Controls

Six out of 21 CBP switch rooms at JFK did not have humidity and temperature sensors. Five rooms with sensors had temperatures that exceeded temperature ranges established by DHS policy. The humidity control readings for these five rooms were within the ranges set by DHS policy.

According to the *DHS 4300A Sensitive Systems Handbook*:

- Humidity should be at a level between 35 percent and 65 percent.
- Temperatures in computer storage areas should be between 60 and 70 degrees Fahrenheit.

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Inadequate Equipment

CBP did not have a large enough box in the office storage area to contain one of its telecommunication switches. As a result, the box could not properly close. Figure 10 shows the box and the telecommunication switches mounted unprotected, beside the box.

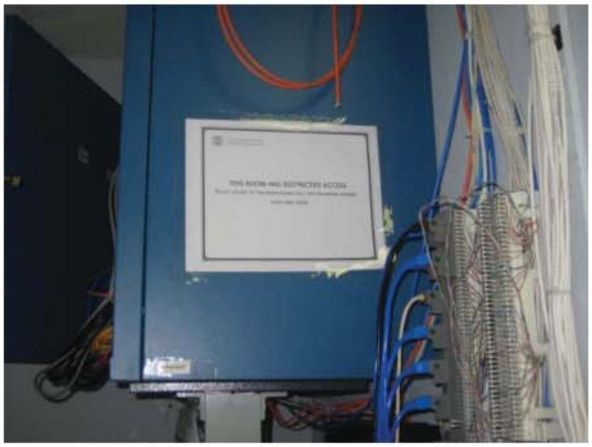


Figure 10- Unlocked Switch Box

According to DHS Sensitive System Policy Directive 4300A:

> Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.

Without adequate physical security controls, unauthorized individuals may gain access to sensitive TSA hardware.

Technical Controls

CBP's implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, identified vulnerabilities on CBP servers were not being resolved in a timely manner.

Patch Management

In February 2014, we observed CBP staff perform vulnerability scans on the three servers located at JFK. [redacted] Table 3 provides the number of vulnerabilities identified by server.

Table 3- Critical, High, and Medium Vulnerabilities

CBP Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]

According to the *DHS 4300A Sensitive Systems Handbook*:

> Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction stated in the Information Security Vulnerability Management message published by the DHS Security Operations Center.

Server vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of CBP data. CBP IT Security officials reviewed the technical results for the three servers and immediately began corrective actions to resolve the two critical vulnerabilities.

Management Controls

CBP's implementation of management controls for the CCTV cameras and surveillance room systems operating at JFK did not conform fully to DHS policies. For example, CBP had not designated the CCTV cameras and surveillance room systems as DHS IT systems. As a result, CBP had not performed the security authorization processes and privacy requirements over the newly installed physical security measures at JFK terminals.

CCTV Cameras and Surveillance Room

CBP did not designate the JFK CCTV cameras and surveillance monitoring room systems as DHS IT systems nor did it implement the applicable, operational, technical, and managerial controls for these JFK systems. CBP failed to designate the cameras and surveillance monitoring room equipment as DHS IT systems, as required by *DHS Sensitive Systems Policy Directive 4300A,* sections 1.4.7 and 1.4.8.

We observed several CCTV cameras in the Terminal 4 area of the CBP passenger processing primary and secondary locations.[4] Figure 11 shows CBP's primary passenger processing area.

[4] Primary processing is the first point of examination of passengers by a CBP officer. Those passengers selected for further examination are referred to a secondary processing point for a more thorough inspection.

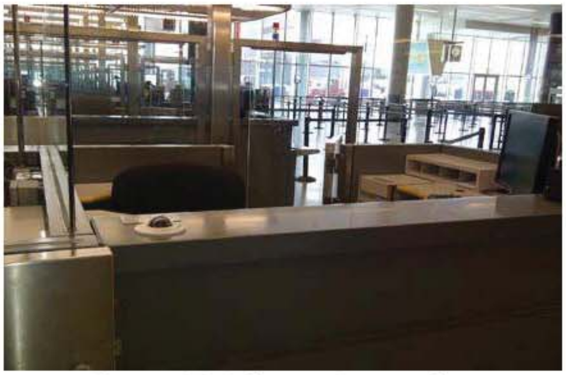


Figure 11-Primary Processing

In 2013, CBP acquired newly renovated space at JFK that included CCTV cameras and a CBP surveillance monitoring room containing IT equipment. The CBP Command and Control Center employees use the cameras to assess threats signaled by alarm events and for surveillance by CBP airport security to monitor activity both inside and outside the terminal.[5] CBP requires a secondary CCTV system that allows officers to monitor detainees in the secondary processing areas, interview rooms, holding rooms, and expedited voluntary removal rooms. CBP officials estimate that approximately 300 cameras are throughout viewable areas within CBP primary passenger processing, secondary passenger processing, interview rooms, and holding rooms. CBP officials operate and monitor the cameras from a CBP secured surveillance monitoring room. Only CBP officials have permission to view cameras observing operations in secondary processing areas. Figure 12 shows the CBP surveillance monitoring room.

[5] Command and Control Center is a station centrally located within the airport's Federal Inspection Service Areas, where CBP systems are monitored.

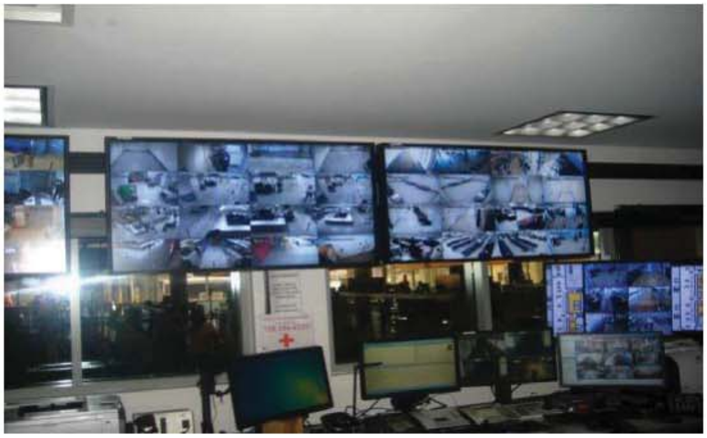


Figure 12- Views of CBP Surveillance Monitoring

The cameras record audio and visual interactions between CBP officers and passengers. However, the Airport Authority owns the CCTV cameras. Since CBP information is being stored, transmitted, and monitored on this system, CBP has the requirement to designate the cameras and surveillance monitoring room as DHS IT systems. By not designating the cameras and surveillance monitoring room as an IT system, CBP did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A.

According to *DHS Sensitive Systems Policy Directive 4300A*:

> A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf.

DHS Sensitive Systems Policy Directive 4300A states that the CISO shall ensure that all information systems are formally assessed through a comprehensive evaluation of management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates PII. Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The

PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

PII includes photographic facial images and any other unique identifying number or characteristic.

Among other things, OMB M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when it uses IT to collect new information.

CBP has not fulfilled security authorization or privacy requirements for the cameras and surveillance equipment at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put the information at risk, and may lead to violations of U.S. privacy laws and DHS policy.

Recommendations:

We recommend that the CBP CIO

Recommendation #7:

Maintain the temperatures of servers and switch rooms within the established temperature ranges.

Recommendation #8:

Secure CBP information technology equipment from unauthorized access.

Recommendation #9:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #10:

Designate the surveillance systems as CBP/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS GAO OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #7 through #10 and has provided details on corrective actions to address each recommendation.

Recommendation #7:

DHS concurred with recommendation 7. CBP's response outlines its plans to install humidity and temperatures sensors. CBP agrees to set humidity and temperatures to the recommended range per the DHS 4300A Sensitive Systems Handbook. These corrective actions are expected to be completed by December 31, 2014. We believe that such efforts are good steps toward addressing our recommendation. We look forward to receiving additional documentation on CBP's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #8:

DHS concurred with recommendation 8. CBP's response outlines its plans to obtain a lockable rack large enough to secure the identified telecommunication switch from unauthorized access. This corrective action is expected to be completed by January 31, 2015. We look forward to receiving notification from

CBP that the lockable rack has been installed and in use. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #9:

DHS concurred with recommendation 9. CBP officials plan to review the OIG reported vulnerabilities to ensure that all critical and high vulnerabilities are addressed. CBP's review is expected to be completed by February 28, 2015. Although, this response appears to address critical and high vulnerabilities, it does not address any corrective actions for the remaining vulnerabilities identified in our report. We look forward to learning more about CBP's actions on this recommendation in the near future. This recommendation will remain open and unresolved pending verification of corrective actions and supporting documentation for all vulnerabilities identified.

Recommendation #10:

Although DHS concurred with recommendation 10, it does not appear that its concurrence addressed all of the concerns noted in our recommendation. Specifically, CBP does not take full ownership of all of the CCTV cameras. CBP agrees that it needs to perform a PTA for CBP's collection and use of the CCTV information. Additionally, CBP plans to determine whether further privacy compliance coverage is warranted through an update to DHS/CBP's current CCTV PIA.

However, CBP only plans to perform the PTA and PIA on the cameras it owns. Although the Port Authority owns some of the cameras in CBP's areas, these cameras and surveillance systems also store, transmit, and monitor CBP information. As a result, CBP has the requirement to designate the cameras and surveillance monitoring room systems as DHS IT systems and to perform required security and privacy reviews. By not designating the cameras and surveillance monitoring room systems as a DHS IT system, CBP did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

DHS/CBP did not provide sufficient corrective actions for our review. We look forward to reviewing CBP's progress in the future. However, this recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

ICE Did Not Comply Fully with DHS Sensitive Systems Policies

ICE did not comply fully with DHS operational, technical and management policies for its servers and switches operating at JFK. Specifically, ICE server and telecommunication rooms did not contain humidity and temperature sensors. Also, ICE had not implemented identified information security patches to its servers. Additionally, ICE did not designate the CCTV cameras and surveillance monitoring equipment as DHS IT systems nor did it implement the applicable, operational, technical, and managerial controls for these JFK systems. Finally, ICE CCTV cameras and surveillance system did not function properly or reliably. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by ICE at JFK.

Operational Controls

ICE server rooms and communications closets at JFK were clean and well maintained. However, onsite implementation of operations controls did not conform fully to DHS policies. For example, the ICE servers and switch rooms did not have the appropriate humidity and temperature control devices to measure and record humidity and temperature ranges as required by DHS policies.

Humidity and Temperature Controls

The ICE servers and switch rooms did not contain any humidity and temperature sensors.

According to the *DHS 4300A Sensitive Systems Handbook*:

- Humidity should be at a level between 35 percent and 65 percent.
- Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit.

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Technical Controls

Patch Management

ICE implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, vulnerabilities identified on ICE servers were not being resolved in a timely fashion. Table 4 provides the number of critical, high, and medium level vulnerabilities identified for each server.

Table 4- Critical, High, and Medium Vulnerabilities

ICE Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	0	1	6
2	0	2	4
3	0	0	2
4	0	1	2
Total	0	4	14

According to the DHS 4300A Sensitive Systems Handbook:

> Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction as stated in the Information Security Vulnerability Management message published by the DHS Security Operations Center.

Server vulnerabilities that are not mitigated could compromise the confidentiality, integrity, and availability of ICE data. If the identified security vulnerabilities are not addressed, they could lead to the introduction of malicious code or unauthorized access to ICE information systems.

Management Controls

CCTV and Surveillance Systems

ICE's implementation of management controls over its CCTV cameras and surveillance systems for the physical security requirements at JFK did not conform fully to DHS policies. Specifically, in April 2010, ICE acquired space at Terminal 4, JFK for the Joint Narcotics and Smuggling Unit. This space includes CCTV cameras, a surveillance monitor, and a digital video receiver. Figure 13 shows the ICE surveillance monitor.

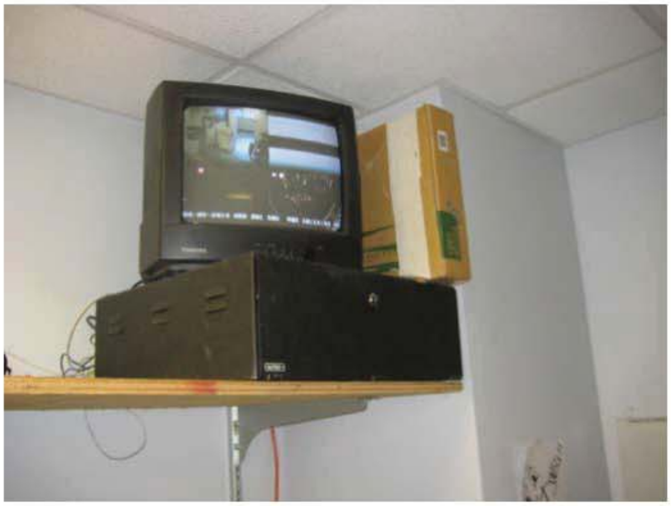


Figure 13- ICE's Surveillance Monitor

However, ICE failed to designate the cameras and surveillance monitor as a DHS IT system as required by *DHS Sensitive Systems Policy Directive 4300A,* sections 1.4.7 and 1.4.8.

ICE officials stated that they did not designate the cameras and surveillance monitor as a DHS IT system because the Airport Authority owned the system. Since ICE information is being stored, transmitted, and monitored on this system, then ICE has the requirement to designate the cameras and surveillance monitor as a DHS IT system. By not designating the cameras and surveillance monitoring room systems as a DHS IT system, ICE did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming

these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

Additionally, two of four CCTV cameras at the Terminal 4 Joint Narcotics and Smuggling Unit communication room were not working during our site visit. The surveillance system monitor connected to the CCTV cameras did not properly display all captured images. ICE officials stated that the cameras had not worked for a period of time but the surveillance system monitor was operating properly 3 days prior to our visit. The ICE officials indicated that they would request camera repairs.

According to *DHS Sensitive Systems Policy Directive 4300A*:

> A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf.

DHS Sensitive Systems Policy Directive 4300A states that the CISO shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates PII. Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

PII includes photographic facial images and any other unique identifying number or characteristic.

Also, OMB M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when they use IT to collect new information.

ICE has not fulfilled security authorization or privacy requirements for the cameras and surveillance equipment at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put the information at risk, and lead to violations of U.S. privacy laws and DHS policy.

Lastly, the identified vulnerabilities on ICE CCTV cameras and surveillance monitor degrade physical security for ICE and law enforcement staff members.

Recommendations

We recommend that the ICE CIO:

Recommendation #11:

Obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Recommendation #12:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #13:

Designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Recommendation #14:

Upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit at JFK.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS GAO OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #11 through #14 and has already taken actions to resolve reported deficiencies.

Recommendation #11:

DHS concurred with recommendation 11. The ICE OCIO plans to to obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300A Sensitive Systems Handbook. ICE estimated the corrective actions would be completed by October 31, 2014. We look forward to receiving additional documentation on ICE's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #12:

DHS concurred with recommendation 12. The ICE OCIO plans to remediate vulnerabilities as they are identified, or within timeframes specified by the DHS Security Operations Center messages. ICE expects this process to be an ongoing effort, however, with an estimated completion date of December 31, 2014. We look forward to receiving additional documentation on ICE's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #13:

DHS concurred with recommendation 13. ICE agreed with the intent of this recommendation for the the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ICE's OCIO and Homeland Security Investigations plans to coordinate and designate the surveillance systems as ICE/DHS IT systems. ICE also plans to implement applicable DHS management, technical, operational controls, and privacy controls and reviews. ICE anticipates completing corrective actions for this recommendation by June 30, 2015. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #14:

DHS concurred with recommendation 14. ICE's Homeland Security Investigations, with assistance from the ICE OCIO, plans to assess the feasibility to upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ICE officials estimate the completion date of the feasibility study by June 30, 2015. Although this response addresses part our recommendation, it does not outline any corrective actions for the repair of the inoperable CCTV cameras and surveillance system. We look forward to reviewing ICE's progress in the future. This recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

USSS Fully Complied with DHS Sensitive Systems Policies

USSS fully complied with DHS operational, technical, and management operational policies for its telecommunication room at JFK. We audited IT security controls of the USSS telecommunication room located at the JFK on-site building number 75. This location had a DHS OneNet connection and a network switch device. The telecommunications room was clean and well maintained. Visitor's logs were also maintained. Humidity and temperature sensor readings were within DHS policy guidelines. Since, the JFK location did not have an on-site server, vulnerability scans were not applicable.

Department's Nonconcurrence

Based on the Department's nonconcurrence with recommendation #6, we have added two additional recommendations that were not part of our draft report. Specifically, we recommend that the DHS CIO:

Recommendation #15:

Coordinate steps with DHS components located at JFK, to ensure their compliance with DHS Sensitive Systems Policy Directive 4300A, Section 1.4.8, and to designate the JFK CCTV cameras and surveillance systems as DHS IT systems.

We also recommend that the DHS Chief Privacy Officer:

Recommendation #16:

Require DHS components located at JFK to prepare PTAs and, as applicable, PIAs for the JFK CCTV cameras and surveillance systems as directed by privacy laws and policy.

Appendix A
Objectives, Scope, and Methodology

The DHS Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

This audit is part of a program to evaluate, on an ongoing basis, the implementation of DHS technical and information security policies and procedures at DHS sites. The objective of this program is to determine the extent to which critical DHS sites comply with the Department's technical and information security policies and procedures, according to *DHS Sensitive Systems Policy Directive 4300A* and its companion document, the *DHS 4300A Sensitive Systems Handbook*. Our primary focus was on evaluating the security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS IT infrastructure at this site. For example, we recorded humidity and temperature at different locations in the server rooms, and then averaged these readings. We also recorded humidity and temperature readings obtained from component sensors that existed in the rooms during fieldwork. We then compared these readings with DHS guidance.

We coordinated the implementation of this technical security evaluation program with the DHS Chief Information Security Officer. We interviewed TSA, CBP, ICE, and USSS, and other staff. We conducted site visits of TSA, CBP, ICE, and USSS facilities at and near JFK. We compared the DHS IT infrastructure that we observed onsite with the documented standards provided by the auditees.

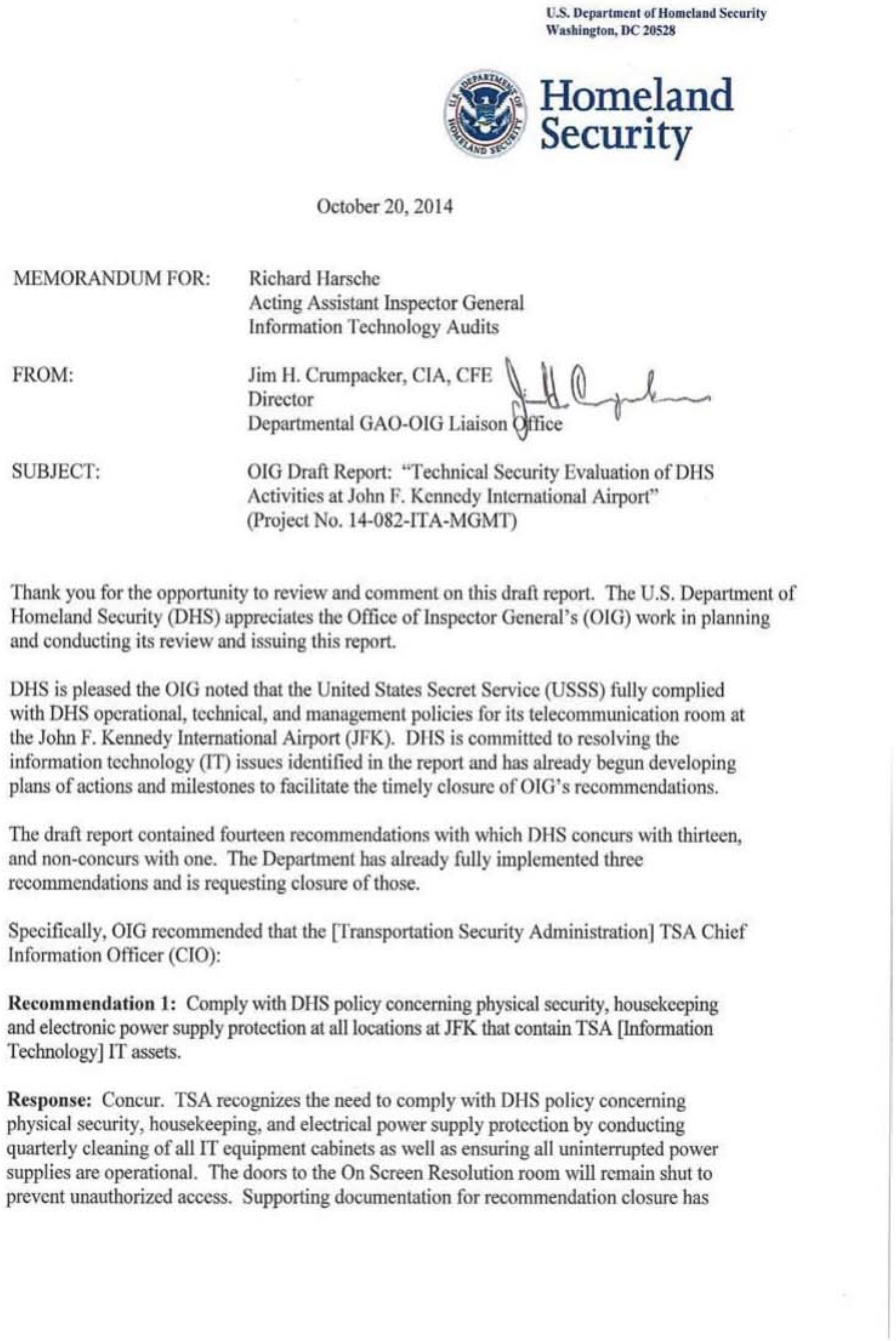
We reviewed the Information Assurance Compliance System documentation, such as the authority-to-operate letter, contingency plans, and system security plans. Additionally, we reviewed guidance provided by DHS to its components in the areas of system documentation, patch management, and wireless security. We also reviewed applicable DHS and components' policies and procedures, as well as Government-wide guidance. We gave briefings and presentations to DHS staff concerning the results of fieldwork and the information summarized in this report.

We conducted this performance audit between November 2013 and April 2014 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable

basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

We appreciate the efforts of DHS management and staff to provide the information and access necessary to accomplish this audit. The principal OIG points of contact for the audit are Richard Harsche, Acting Assistant Inspector General for Information Technology Audits, (202) 254-4100, and Sharon Huiswoud, Director, Information Systems Division, (202) 254-5451. Appendix D contains a major OIG contributors listing.

Appendix B
Management Comments to the Draft Report



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 20, 2014

MEMORANDUM FOR:	Richard Harsche Acting Assistant Inspector General Information Technology Audits
FROM:	Jim H. Crumpacker, CIA, CFE Director Departmental GAO-OIG Liaison Office
SUBJECT:	OIG Draft Report: "Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport" (Project No. 14-082-ITA-MGMT)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG) work in planning and conducting its review and issuing this report.

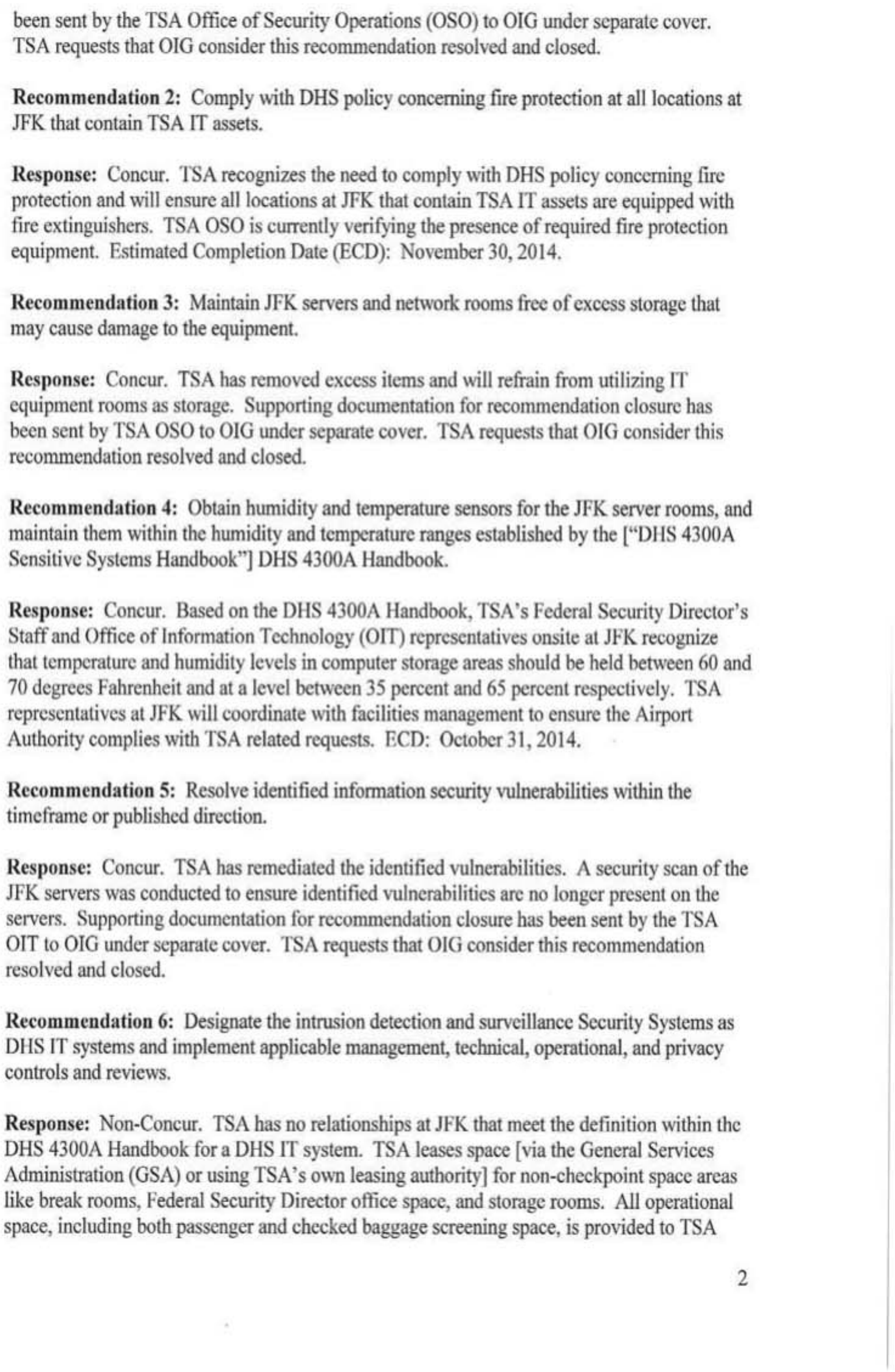
DHS is pleased the OIG noted that the United States Secret Service (USSS) fully complied with DHS operational, technical, and management policies for its telecommunication room at the John F. Kennedy International Airport (JFK). DHS is committed to resolving the information technology (IT) issues identified in the report and has already begun developing plans of actions and milestones to facilitate the timely closure of OIG's recommendations.

The draft report contained fourteen recommendations with which DHS concurs with thirteen, and non-concurs with one. The Department has already fully implemented three recommendations and is requesting closure of those.

Specifically, OIG recommended that the [Transportation Security Administration] TSA Chief Information Officer (CIO):

Recommendation 1: Comply with DHS policy concerning physical security, housekeeping and electronic power supply protection at all locations at JFK that contain TSA [Information Technology] IT assets.

Response: Concur. TSA recognizes the need to comply with DHS policy concerning physical security, housekeeping, and electrical power supply protection by conducting quarterly cleaning of all IT equipment cabinets as well as ensuring all uninterrupted power supplies are operational. The doors to the On Screen Resolution room will remain shut to prevent unauthorized access. Supporting documentation for recommendation closure has



been sent by the TSA Office of Security Operations (OSO) to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 2: Comply with DHS policy concerning fire protection at all locations at JFK that contain TSA IT assets.

Response: Concur. TSA recognizes the need to comply with DHS policy concerning fire protection and will ensure all locations at JFK that contain TSA IT assets are equipped with fire extinguishers. TSA OSO is currently verifying the presence of required fire protection equipment. Estimated Completion Date (ECD): November 30, 2014.

Recommendation 3: Maintain JFK servers and network rooms free of excess storage that may cause damage to the equipment.

Response: Concur. TSA has removed excess items and will refrain from utilizing IT equipment rooms as storage. Supporting documentation for recommendation closure has been sent by TSA OSO to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 4: Obtain humidity and temperature sensors for the JFK server rooms, and maintain them within the humidity and temperature ranges established by the ["DHS 4300A Sensitive Systems Handbook"] DHS 4300A Handbook.

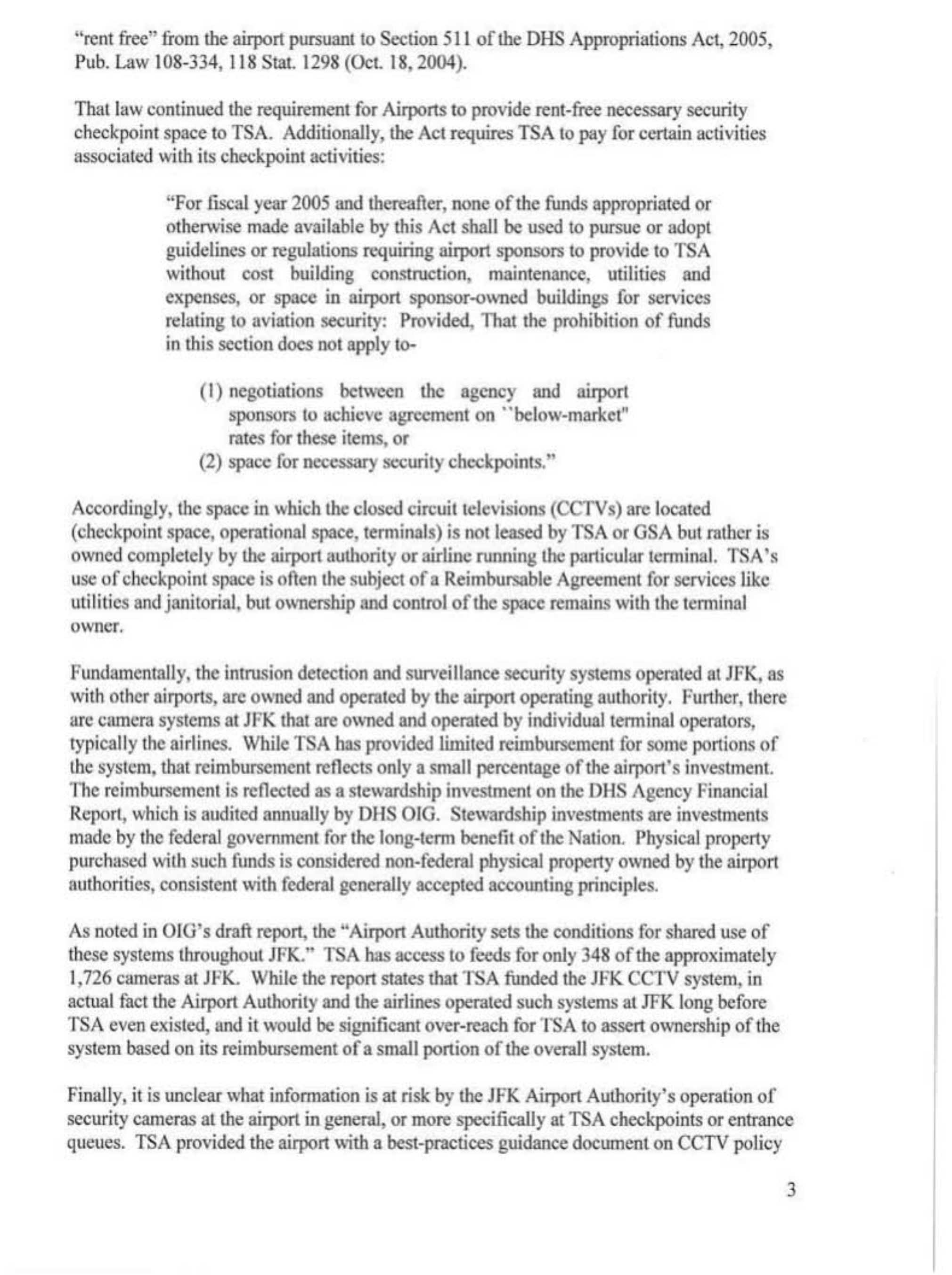
Response: Concur. Based on the DHS 4300A Handbook, TSA's Federal Security Director's Staff and Office of Information Technology (OIT) representatives onsite at JFK recognize that temperature and humidity levels in computer storage areas should be held between 60 and 70 degrees Fahrenheit and at a level between 35 percent and 65 percent respectively. TSA representatives at JFK will coordinate with facilities management to ensure the Airport Authority complies with TSA related requests. ECD: October 31, 2014.

Recommendation 5: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. TSA has remediated the identified vulnerabilities. A security scan of the JFK servers was conducted to ensure identified vulnerabilities are no longer present on the servers. Supporting documentation for recommendation closure has been sent by the TSA OIT to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 6: Designate the intrusion detection and surveillance Security Systems as DHS IT systems and implement applicable management, technical, operational, and privacy controls and reviews.

Response: Non-Concur. TSA has no relationships at JFK that meet the definition within the DHS 4300A Handbook for a DHS IT system. TSA leases space [via the General Services Administration (GSA) or using TSA's own leasing authority] for non-checkpoint space areas like break rooms, Federal Security Director office space, and storage rooms. All operational space, including both passenger and checked baggage screening space, is provided to TSA



"rent free" from the airport pursuant to Section 511 of the DHS Appropriations Act, 2005, Pub. Law 108-334, 118 Stat. 1298 (Oct. 18, 2004).

That law continued the requirement for Airports to provide rent-free necessary security checkpoint space to TSA. Additionally, the Act requires TSA to pay for certain activities associated with its checkpoint activities:

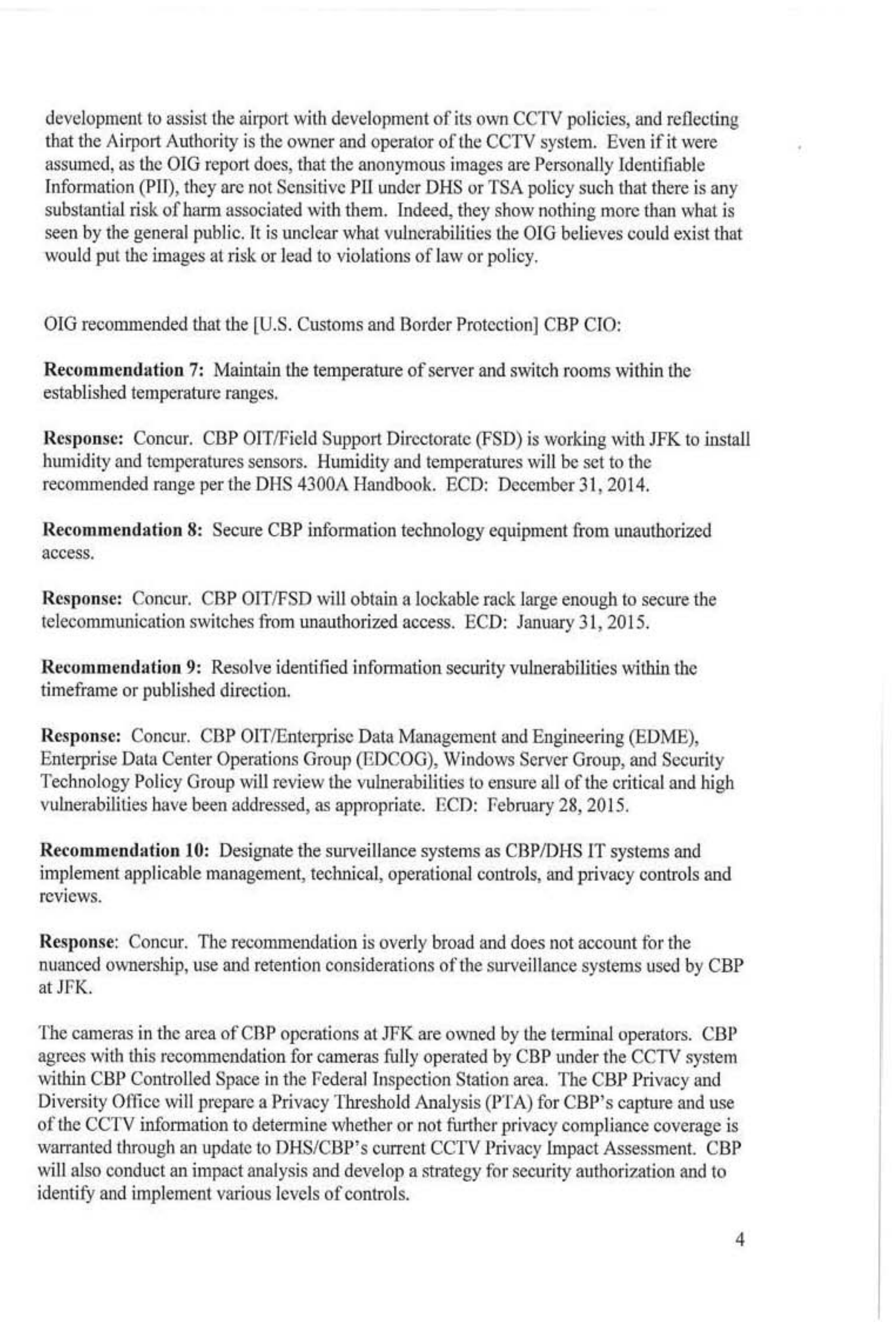
> "For fiscal year 2005 and thereafter, none of the funds appropriated or otherwise made available by this Act shall be used to pursue or adopt guidelines or regulations requiring airport sponsors to provide to TSA without cost building construction, maintenance, utilities and expenses, or space in airport sponsor-owned buildings for services relating to aviation security: Provided, That the prohibition of funds in this section does not apply to-
>
> (1) negotiations between the agency and airport sponsors to achieve agreement on ``below-market" rates for these items, or
> (2) space for necessary security checkpoints."

Accordingly, the space in which the closed circuit televisions (CCTVs) are located (checkpoint space, operational space, terminals) is not leased by TSA or GSA but rather is owned completely by the airport authority or airline running the particular terminal. TSA's use of checkpoint space is often the subject of a Reimbursable Agreement for services like utilities and janitorial, but ownership and control of the space remains with the terminal owner.

Fundamentally, the intrusion detection and surveillance security systems operated at JFK, as with other airports, are owned and operated by the airport operating authority. Further, there are camera systems at JFK that are owned and operated by individual terminal operators, typically the airlines. While TSA has provided limited reimbursement for some portions of the system, that reimbursement reflects only a small percentage of the airport's investment. The reimbursement is reflected as a stewardship investment on the DHS Agency Financial Report, which is audited annually by DHS OIG. Stewardship investments are investments made by the federal government for the long-term benefit of the Nation. Physical property purchased with such funds is considered non-federal physical property owned by the airport authorities, consistent with federal generally accepted accounting principles.

As noted in OIG's draft report, the "Airport Authority sets the conditions for shared use of these systems throughout JFK." TSA has access to feeds for only 348 of the approximately 1,726 cameras at JFK. While the report states that TSA funded the JFK CCTV system, in actual fact the Airport Authority and the airlines operated such systems at JFK long before TSA even existed, and it would be significant over-reach for TSA to assert ownership of the system based on its reimbursement of a small portion of the overall system.

Finally, it is unclear what information is at risk by the JFK Airport Authority's operation of security cameras at the airport in general, or more specifically at TSA checkpoints or entrance queues. TSA provided the airport with a best-practices guidance document on CCTV policy



development to assist the airport with development of its own CCTV policies, and reflecting that the Airport Authority is the owner and operator of the CCTV system. Even if it were assumed, as the OIG report does, that the anonymous images are Personally Identifiable Information (PII), they are not Sensitive PII under DHS or TSA policy such that there is any substantial risk of harm associated with them. Indeed, they show nothing more than what is seen by the general public. It is unclear what vulnerabilities the OIG believes could exist that would put the images at risk or lead to violations of law or policy.

OIG recommended that the [U.S. Customs and Border Protection] CBP CIO:

Recommendation 7: Maintain the temperature of server and switch rooms within the established temperature ranges.

Response: Concur. CBP OIT/Field Support Directorate (FSD) is working with JFK to install humidity and temperatures sensors. Humidity and temperatures will be set to the recommended range per the DHS 4300A Handbook. ECD: December 31, 2014.

Recommendation 8: Secure CBP information technology equipment from unauthorized access.

Response: Concur. CBP OIT/FSD will obtain a lockable rack large enough to secure the telecommunication switches from unauthorized access. ECD: January 31, 2015.

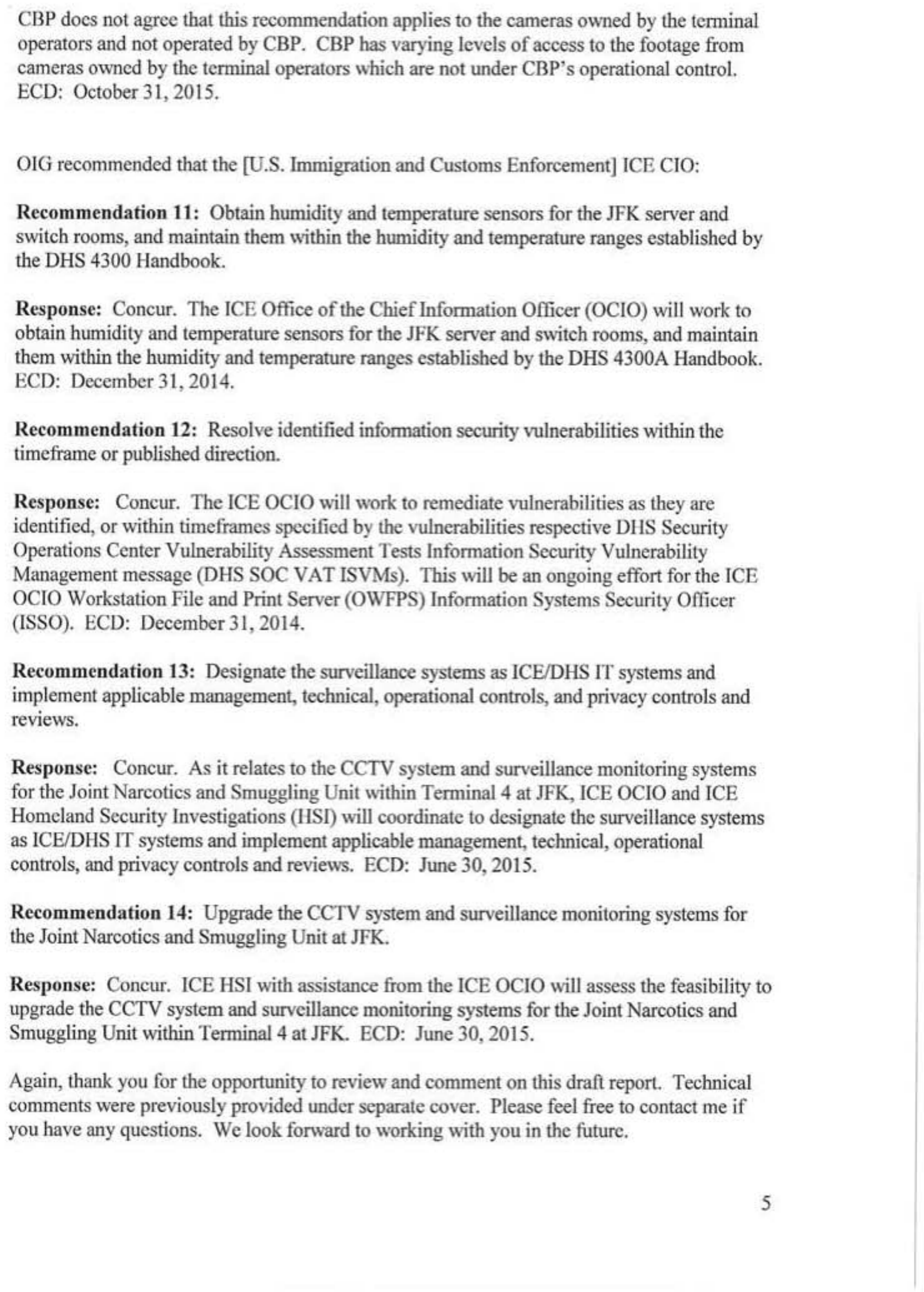
Recommendation 9: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. CBP OIT/Enterprise Data Management and Engineering (EDME), Enterprise Data Center Operations Group (EDCOG), Windows Server Group, and Security Technology Policy Group will review the vulnerabilities to ensure all of the critical and high vulnerabilities have been addressed, as appropriate. ECD: February 28, 2015.

Recommendation 10: Designate the surveillance systems as CBP/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Response: Concur. The recommendation is overly broad and does not account for the nuanced ownership, use and retention considerations of the surveillance systems used by CBP at JFK.

The cameras in the area of CBP operations at JFK are owned by the terminal operators. CBP agrees with this recommendation for cameras fully operated by CBP under the CCTV system within CBP Controlled Space in the Federal Inspection Station area. The CBP Privacy and Diversity Office will prepare a Privacy Threshold Analysis (PTA) for CBP's capture and use of the CCTV information to determine whether or not further privacy compliance coverage is warranted through an update to DHS/CBP's current CCTV Privacy Impact Assessment. CBP will also conduct an impact analysis and develop a strategy for security authorization and to identify and implement various levels of controls.



CBP does not agree that this recommendation applies to the cameras owned by the terminal operators and not operated by CBP. CBP has varying levels of access to the footage from cameras owned by the terminal operators which are not under CBP's operational control. ECD: October 31, 2015.

OIG recommended that the [U.S. Immigration and Customs Enforcement] ICE CIO:

Recommendation 11: Obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Response: Concur. The ICE Office of the Chief Information Officer (OCIO) will work to obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300A Handbook. ECD: December 31, 2014.

Recommendation 12: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. The ICE OCIO will work to remediate vulnerabilities as they are identified, or within timeframes specified by the vulnerabilities respective DHS Security Operations Center Vulnerability Assessment Tests Information Security Vulnerability Management message (DHS SOC VAT ISVMs). This will be an ongoing effort for the ICE OCIO Workstation File and Print Server (OWFPS) Information Systems Security Officer (ISSO). ECD: December 31, 2014.

Recommendation 13: Designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Response: Concur. As it relates to the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK, ICE OCIO and ICE Homeland Security Investigations (HSI) will coordinate to designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews. ECD: June 30, 2015.

Recommendation 14: Upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit at JFK.

Response: Concur. ICE HSI with assistance from the ICE OCIO will assess the feasibility to upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ECD: June 30, 2015.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Appendix C
DHS Activities at JFK Airport

Transportation Security Administration

TSA uses technology to screen passengers and baggage on all departing flights at each of the JFK terminals and to support operation management at nearby office buildings.

We audited IT security controls at the following TSA locations:

- JFK Terminals 1, 2, 4, 5, 7, and 8,
- Office of the Federal Security Director, Jamaica, NY, and
- Office of Federal Air Marshal Service (FAMS), Jamaica, NY.

TSA staff at these locations use the following systems:

- Federal Air Marshal Service Network (FAMSNet) – provides the IT infrastructure to support the FAMS law enforcement mission to help detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews. FAMSNet provides Internet access as well as internal access to FAMS information systems including, but not limited to, email, databases, file sharing, printing, and a number of critical administrative and enforcement related programs. FAMSNet also provides a communication pathway to third-party and Government networks, such as those used by other DHS components, the Federal Aviation Administration, and other State and local law enforcement entities.
- Infrastructure Core System – provides electronic file and print capabilities to the entire TSA user community.
- TSA End User Computing System – provides TSA employees and contractors with desktops, laptops, local printers, mobile devices and other end user computing applications.
- Security Technology Integrated Program – combines many different types of components, including transportation security equipment, servers and storage, software/application products, and databases. Users physically access the transportation security equipment to perform screening or other administrative

functions. TSA's Office of Security Capabilities is the owner of the Security Technology Integrated Program.

- Transportation Security Administration Network (TSANet) – provides connectivity in airports for TSA users. TSANet consists of a geographically-dispersed wide area network and each site's local area network. The networks are connected to the DHS One Network (OneNet) and have been designated a mission essential system.

U.S. Customs and Border Protection

CBP employs over 1,600 staff at JFK to protect the United States from drug and human smugglers, agricultural diseases and pests, and terrorists. CBP personnel also:

- review flight data for terrorist-related activities,
- collect duties, and
- assess fines and civil penalties.

Also, CBP staff at nearby locations use IT assets to perform cargo and outbound passenger review and targeting. In addition, JFK CBP employees operate and maintain the international mail facility.

We audited IT security controls at the following CBP locations:

- JFK Terminals 1, 4, 5, 7, and 8, and
- CBP buildings Number 77 and 250, located in Jamaica, NY.

CBP staff at these locations use the following systems:

- Northeast Field Local Area Network – provides the general support network infrastructure for DHS/CBP users and electronic communications tools, which enables the execution of official duties. The Northeast Field Local Area Network includes 290 geographically dispersed sites using 9,000 devices connected to the OneNet to provide application services to CBP field offices.

- CBP Network Operations Center – maintains the performance, management, and administration of the core network and underlying supporting environment at CBP field site locations. In addition, the center deploys and maintains a network management system and a suite of network devices that collect and report real-time network security information. Further, the center manages the flow of information within interconnected systems in accordance with DHS Sensitive Security Policy.

- Windows 7 PC Client 6.1 – used as the Windows 7 standard desktop image for CBP workstations. Windows 7 PC Client 6.1 consists of a set of standard configurations and installs application software and configures systems according to DHS and CBP technical standards.

- The Windows File and Print System – provides CBP with file and printing services using the Microsoft Windows Server 2008 x 64 platforms.

- Treasury Enforcement Communication System (TECS) – supports enforcement and inspection operations for several components of DHS and is a vital tool for local, State, tribal, and Federal Government law enforcement and intelligence communities.6 TECS includes several subsystems for enforcement, inspection, and intelligence records relevant to the antiterrorist and law enforcement mission of CBP and other Federal agencies.

[6] Formerly known as the Treasury Enforcement Communications System, TECS is no longer an acronym (effective December 19, 2008) and is principally owned and managed by CBP.

U.S. Immigration and Customs Enforcement

The New York ICE Office of the Special Agent in Charge is responsible for the administration and management of all investigative and enforcement activities within its geographical boundaries. Within the New York Special Agent in Charge office, the Homeland Security Investigations Airport Group is responsible for the identification, disruption, and dismantlement of transnational criminal organizations attempting to exploit vulnerabilities within the air transportation system at JFK. The Homeland Security Investigations Airport Group's areas of concern at JFK include:Contraband smuggling,

- Currency smuggling,
- National security,
- Human smuggling/trafficking,
- Sexual tourism,
- Insider threat, and
- Theft and trafficking of cultural heritage and art.

The JFK Office of Professional Responsibility investigates criminal and administrative misconduct committed by ICE and CBP employees and contractors. This office also addresses complaints of people pretending to be ICE and CBP employees or attempted bribery.

We audited IT security controls at the following ICE locations:

- The Special Agent in Charge New York Office, located in Building No. 75,
- Office of Professional Responsibility, located in Building No. 75, and
- Joint Narcotics and Smuggling Unit, located in JFK Terminal 4.

ICE staff at these locations use the following systems:

- Office File and Print Servers – provide workstation, laptop, print services, and file capability to all ICE employees. File servers provide a networked file repository and print servers allow networked printing.

- ICE Communication over Networks – provides support for all network devices and data communications used by ICE and at 287(g) sites.7

- A communication surveillance and analysis system that helps Homeland Security Investigations staff to gather intelligence and collect live data in support of ICE's law enforcement mission. Specifically, the system assembles historical telephone records, monitors telephone and Internet communications, and permits searches of warrant data from online providers. The communication surveillance and analysis system connects to the ICE network infrastructure or on a separate standalone network. This is not a designated mission essential system.

U.S. Secret Service

USSS have nine agents and two administrative personnel located at JFK that report directly to the USSS New York Field Office in Brooklyn, NY. This office is the only USSS office located at an airport.

The agents assigned to the office handle between 750 and 800 arrivals and departures of USSS protected individuals/groups, including Prime Ministers and current and former U.S. Presidents and immediate family members, at JFK and LaGuardia Airports. Each September, the United Nations General Assembly in New York City impacts the JFK Resident Office with over 300 arrivals and departures at JFK and LaGuardia Airports and an additional 42 temporarily assigned agents/officers.

The office also works closely with CBP to seize counterfeit United States currency entering JFK Airport at the passenger and cargo terminals. Since May 2010, DHS seized United States currency totaling over $4 million. The employees of the USSS office use Windows 7, Office 2010, and web—based applications. The service's New York Field Office Technical Operations Squad performs all IT updates, equipment repairs, and installation of new equipment.

[7] The 287(g) program, under the *Immigration and Nationality Act*, as amended, allows a state and local law enforcement entity to receive delegated authority for immigration enforcement within its jurisdiction.

Appendix D
Major Contributors to This Report

Sharon Huiswoud, IT Audit Director
Sharell Grady, IT Audit Manager
Beverly Dale, IT Senior Auditor
Robert Durst, Senior Program Analyst
Frederick Shappee, Senior Program Analyst
Daniel McGrath, Referencer

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
DHS CISO
DHS CISO Audit Liaison
CBP CIO
CBP Audit Liaison
ICE CIO
ICE Audit Liaison
TSA CIO
TSA Audit Liaison
USSS CIO
USSS Audit Liaison
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

Special Assistant to the Inspector General
Office of Inspector General
202-254- (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

From: Balaban, Dorothy
Sent: Friday, November 21, 2014 5:57 PM
To: (b)(6);(b)(7)(C)
Cc:
Subject: OIG's Challenge to SSI

Good Evening,

Attached please find a letter to the Administrator from Inspector General regarding OIG Report – Technical Security Evaluation of DHS Activities at JFK International Airport.

Let me know if you need anything else.

Thanks,

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254- (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

2 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

From: Balaban, Dorothy
Sent: Friday, January 09, 2015 01:26 PM
To: Huiswoud, Sharon
Subject: FW: Memo for Mr. Pistole re JFK Int'l Airport

FYI

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254 (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

From: Balaban, Dorothy
Sent: Wednesday, December 17, 2014 10:22 AM
To: (b)(6);(b)(7)(C)
Subject: Memo for Mr. Pistole re JFK Int'l Airport

Hi (b)(6);(b)(7)(C)

Could you see that Mr. Pistole gets this memo. It will be distributed thru it's normal channels, but I wanted to give Mr. Pistole a heads up.

Have a great holiday.

Thanks,

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254- (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

Requester’s Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

5 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

MEMORANDUM FOR:	The Honorable John Pistole Administrator Transportation Security Administration
FROM:	John Roth Inspector General
SUBJECT:	Follow up to my Challenge Memo to the SSI Markings to draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport-Sensitive Security Information*

I am writing to follow up on the memo I sent you on November 19, 2014, regarding my challenge to Sensitive Security Information (SSI) markings to our draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport*. We are preparing to issue this report as final. However, I am concerned that I have not heard back from you regarding my request to remove the SSI markings from our report so that we may issue it in its entirety in the public domain.

In response to a law passed by the Congress in 2006, the Department revised DHS Management Directive (MD) 11056.1 to require TSA to ensure a timely SSI review of public requests for release of information. Given MD 11056.1, section V.B.7's requirement for timely SSI reviews in response to requests from the public, we hoped that TSA would approach our SSI appeal from a fellow component with similar diligence, especially since TSA is aware of our deadlines. We are disappointed.

In its October 20, 2014, response to our draft report, the Department indicated that several statements within the report were determined to be SSI. I disagree with the markings and submitted my challenge to you in accordance with guidance provided under MD 11056.1.

I again request that you reconsider and remove the SSI markings from our draft report. I recognize the SSI Office's process to identify and safeguard SSI information. However, I believe that improperly marking information in our draft report as SSI impedes our ability to issue reports to the public that are transparent, without unduly restricting information, which is key to accomplishing our mission. Per DHS MD 11056.1, VI.A.3, SSI markings should not be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency.

This report has languished for months because of TSA's sensitivity review. Absent a decision from you, we will be forced to publish a redacted report to meet our timeliness requirements. The report will contain our objections to the redactions. Consistent with our responsibilities under the *Inspector General Act*, we will provide unredacted copies of our report to Congressional Committees with oversight and appropriations responsibility for the Department of Homeland Security.

I appreciate your personal attention to this matter and I await your response. Should you have any questions, please call me.

Attachment

From: Harsche, Richard
Sent: 20 Nov 2014 19:05:21 -0500
To: Balaban, Dorothy
Cc: Tsang, Chiu-Tong
Subject: Re: Anticipated SSI Program Schedules and SSI Review 14-0826

Dottie,
I noticed a small typo on page two. In the last sentence of the second bullet, the word "we" should be removed.
Rick

From: Balaban, Dorothy
Sent: Thursday, November 20, 2014 05:57 PM
To: Harsche, Richard
Cc: Tsang, Chiu-Tong
Subject: RE: Anticipated SSI Program Schedules and SSI Review 14-0826

Here's the memo to Pistole. Do you want me to send it to him, or do you want to send it to your counterpart?

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254 (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

From: Harsche, Richard
Sent: Thursday, November 20, 2014 2:03 PM
To: Balaban, Dorothy
Subject: FW: Anticipated SSI Program Schedules and SSI Review 14-0826

Dottie,
This information was provided by the Department for our SSI challenge memo. Please notice the email and cc information.
Rick

From: Eyl, Nancy
Sent: Thursday, November 20, 2014 1:11 PM
To (b)(6)
Cc: Harsche, Richard; Mobbs, Michael
Subject: Re: Anticipated SSI Program Schedules and SSI Review 14-0826

From: Harsche, Richard
Sent: 20 Nov 2014 18:24:31 -0500
To: Balaban, Dorothy;Tsang, Chiu-Tong
Subject: RE: Anticipated SSI Program Schedules and SSI Review 14-0826

Agree. Thanks, Dottie.
Rick

From: Balaban, Dorothy
Sent: Thursday, November 20, 2014 6:05 PM
To: Tsang, Chiu-Tong; Harsche, Richard
Subject: RE: Anticipated SSI Program Schedules and SSI Review 14-0826

Will do. No problem.

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254 (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

From: Tsang, Chiu-Tong
Sent: Thursday, November 20, 2014 6:05 PM
To: Balaban, Dorothy; Harsche, Richard
Subject: Re: Anticipated SSI Program Schedules and SSI Review 14-0826

Dottie,

Since the memo is going to the TSA Director, maybe it's appropriate if you can send it out, if you don't mind?

Thanks.

Tom

Tom Tsang
Director, Information Security Audit Division
DHS OIG
Office-202-254 (b)(6);(b)(7)(C)
BlackBerry-202-369 (b)(6);(b)(7)(C)
Sent from my BlackBerry Wireless Handheld

From: Balaban, Dorothy
Sent: Thursday, November 20, 2014 05:57 PM
To: Harsche, Richard
Cc: Tsang, Chiu-Tong
Subject: RE: Anticipated SSI Program Schedules and SSI Review 14-0826

Here's the memo to Pistole. Do you want me to send it to him, or do you want to send it to your counterpart?

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254 (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

From: Harsche, Richard
Sent: Thursday, November 20, 2014 2:03 PM
To: Balaban, Dorothy
Subject: FW: Anticipated SSI Program Schedules and SSI Review 14-0826

Dottie,
This information was provided by the Department for our SSI challenge memo. Please notice the email and cc information.
Rick

From: Eyl, Nancy
Sent: Thursday, November 20, 2014 1:11 PM
To (b)(6)
Cc: Harsche, Richard; Mobbs, Michael
Subject: Re: Anticipated SSI Program Schedules and SSI Review 14-0826

(b)(6)

Thank you for writing. I am forwarding your message to our AIG for IT audits. Rick Harsche has a better handle on this than I do.

Best
Nancy

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

5 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

From: Crumpacker, Jim
Sent: 17 Mar 2017 09:04:42 -0400
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Any update yet? March 31, 2017 is fast approaching (smile). Thank you. v/r Jim

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office
U.S. Department of Homeland Security

(202) 447 (b)(7)(C); office)
(202) 262 (b)(6) cell)

"Liaison = Relationships + Communication"

IMPORTANT: This e-mail, including all attachments, constitutes Federal Government records and property that is intended only for the use of the individual or entity to which it is addressed. It may also contain information that is privileged, confidential, or otherwise protected from disclosure under applicable law. If the reader of this e-mail transmission is not the intended recipient or the employee or agent responsible for delivering the transmission to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this e-mail or its contents is strictly prohibited. If you have received this e-mail in error, please notify the sender by responding to the e-mail and then delete the e-mail immediately.

From: Crumpacker, Jim
Sent: Tuesday, February 21, 2017 7:27 PM
To: Balaban, Dorothy (b)(7)(C);(b)(6) @oig.dhs.gov>
Subject: Re: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Dottie:

Any word on this yet? I would like to get this resolved before the end of the next semi-annual reporting period (3/31/2017).

Also, does the IG anticipate that this report will come up during his congressional hearing about TSA in early March? If so, in what regard (i.e., the CCTV disagreement and/or the SSI marking issue)? Any insights appreciated. Thank you.

Jim

From: Crumpacker, Jim
Sent: Friday, February 17, 2017 09:26 AM Eastern Standard Time
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

?

From: Balaban, Dorothy
Sent: Wednesday, February 1, 2017 11:38 AM
To: Crumpacker, Jim (b)(7)(C);(b)(6) @HQ.DHS.GOV>
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

I'll chat with the IG after the hearing and let you know.

Dottie

From: Crumpacker, Jim
Sent: Wednesday, February 01, 2017 11:25:16 AM
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Dottie: FYI, I hope the hearing on "Empowering the Inspectors General" went well this morning. Unfortunately, I was not able to watch it due to competing priorities. BTW, I've still not heard anything from the IG concerning this non-concurrence. Know he has been extremely busy. Will continue to stand by. v/r Jim

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office
U.S. Department of Homeland Security

(202) 447(b)(7)(C); (office)
(202) 262 (b)(6) (cell)

"Liaison = Relationships + Communication"

IMPORTANT: This e-mail, including all attachments, constitutes Federal Government records and property that is intended only for the use of the individual or entity to which it is addressed. It may also contain information that is privileged, confidential, or otherwise protected from disclosure under applicable law. If the reader of this e-mail transmission is not the intended recipient or the employee or agent responsible for delivering the transmission to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this e-mail or its contents is strictly prohibited. If you have received this e-mail in error, please notify the sender by responding to the e-mail and then delete the e-mail immediately.

From: Crumpacker, Jim
Sent: Tuesday, January 24, 2017 4:10 PM
To: Balaban, Dorothy (b)(7)(C);(b)(6) @oig.dhs.gov) (b)(7)(C);(b)(6) @oig.dhs.gov>

Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

FYI, I left you a phone message about this earlier today. Just following up to determine if OIG has any feedback. Need to package and move forward soon. Please advise. Thank you. Jim

From: Crumpacker, Jim
Sent: Monday, January 23, 2017 10:59 AM
To: Balaban, Dorothy (b)(7)(C);(b)(6) @oig.dhs.gov (b)(7)(C);(b)(6) @oig.dhs.gov>
Subject: FW: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Dottie: Attached forwarded for OIG "fact check," etc., as we just telephonically discussed. Thank you in advance. v/r Jim

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office
U.S. Department of Homeland Security

(202) 447 (b)(7)(C);(b)(6) ffice)
(202) 262 ell)

"Liaison = Relationships + Communication"

IMPORTANT: This e-mail, including all attachments, constitutes Federal Government records and property that is intended only for the use of the individual or entity to which it is addressed. It may also contain information that is privileged, confidential, or otherwise protected from disclosure under applicable law. If the reader of this e-mail transmission is not the intended recipient or the employee or agent responsible for delivering the transmission to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this e-mail or its contents is strictly prohibited. If you have received this e-mail in error, please notify the sender by responding to the e-mail and then delete the e-mail immediately.

From (b)(7)(C);(b)(6)
Sent: Thursday, January 19, 2017 3:52 PM
To: Fulghum, Chip (b)(7)(C);(b)(6) @hq.dhs.gov>
Cc: Crumpacker, Jim (b)(7)(C);(b)(6) @HQ.DHS.GOV> (b)(7)(C);(b)(6)
(b)(7)(C);(b)(6) @tsa.dhs.gov>; Perkins, Susan (b)(6);(b)(7)(C) @tsa.dhs.gov>
Subject: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Good evening,

Please find attached for your review, signature, and transmission to DHS IG Roth, the memorandum memorializing the recent agreement reached between TSA and OIG. The language contained within the document corresponds verbatim to the narrative vetted earlier this month by all parties.

Many thanks for your assistance and that of your staff during the resolution process.

Thank you

(b)(7)(C);(b)(6)
Information Management Specialist
Transportation Security Administration
Office of the Administrator
Office of the Executive Secretariat
E7-105-S
Phone: 571-2
Fax: 571-227 (b)(7)(C);(b)(6)

Requester's Name: Shawn Musgrave

FOIA/PA NO.: 2015-087

9 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

Requester's Name: Shawn Musgrave

2015-087

2 PAGE(S) OF DOCUMENT(S)

WITHHELD IN FULL (WIF)

EXEMPTIONS CITED

(b)(5)

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

MEMORANDUM FOR: The Honorable Chip Fulghum
Acting Under Secretary for Management

FROM: John Roth
Inspector General

SUBJECT: *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport*

Attached for your information is our final report, *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport*. This report contains findings and recommendations for improving security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS information technology infrastructure at this airport.

The procedural history of this report elicits an unfortunate commentary on the manner in which the Department handles these matters and bears review:

- We provided a draft of this report on July 22, 2014 to the Chief Information Officer for review. Pursuant to *Department of Homeland Security Directive 077-01, Follow-up, and Resolution for Office of Inspector General Report Recommendations*, we asked for agency comments, including a sensitivity review, within 30 days of receipt of the draft. This would have made the report due on or about August 22, 2015. Almost a week later, on August 27, 2014, the DHS Chief of Staff requested an extension to provide a response and technical comments. I granted the extension until September 17, 2014.

- On October 20, 2014, nearly 60 days after the original due date for agency comments, the Departmental GAO-OIG Liaison Office finally conveyed to us TSA's response to our request for a sensitivity review by marking several passages in the report as SSI. I disagree with this determination.

- On November 19, 2014, I sent a formal challenge memo to TSA Administrator John Pistole and copied SSI Program Chief Doug Blair, expressing my disagreement. Administrator Pistole had authority over all TSA programs and operations, including oversight of the SSI programs.

- Having received no reply, on December 16, 2014, I wrote to Administrator Pistole a second time, noting that this report had languished as a result of TSA's sensitivity review and again requesting that he remove the SSI markings from the report. As with the November 19, 2014 letter, I received no reply.

- Finally, on January 13, 2015, over five months after submitting the report for sensitivity review, and two months after writing to Administrator Pistole, I received a decision, not from the Acting TSA Administrator, but from the head of the SSI program office—the very same office that initially and improperly marked the information as SSI. Not surprisingly, the office affirmed its original redactions to the report.

I am disappointed in both the substance of the decision as well as its lack of timeliness. In 2006, Congress, concerned about delays in appeals of this nature, directed the Department to revise MD 11056.1 to require TSA to ensure timely SSI reviews of public requests for release of information. Given the clear requirement in MD 11056.1 for timely SSI reviews in response to requests from the public, we hoped that TSA would approach an SSI appeal from a fellow component with similar diligence, especially since TSA was aware of our deadlines. Now, to meet our reporting requirement, we are compelled to publish a redacted report with SSI markings and will again appeal the SSI program office's decision to the Acting TSA Administrator.

I believe that this report should be released in its entirety in the public domain. I challenged TSA's determination because this type of information has been disclosed in other reports without objection from TSA, and because the language marked SSI reveals generic, non-specific vulnerabilities that are common to virtually all systems and would not be detrimental to transportation security. Our ability to issue reports that are transparent, without unduly restricting information, is key to accomplishing our mission. Congress, when it passed the *Reducing Over-Classification Act* in 2010, found that over-classification "interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information."

Consistent with our responsibilities under the *Inspector General Act*, we will provide unredacted copies of our report to appropriate Congressional Committees with oversight and appropriation responsibility for the Department of Homeland Security. We will post a redacted version of the report on our website pending a decision from the Acting TSA Administrator.

I appreciate your attention to this matter. Should you have any questions, please call me, or your staff may contact Sondra McCauley, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4041.

Attachments

cc: Melvin Carraway, Acting Administrator, Transportation Security Administration

From: Balaban, Dorothy
Sent: 17 Mar 2017 13:37:34 +0000
To: Roth, John
Subject: FW: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

FYI

From: Crumpacker, Jim
Sent: Friday, March 17, 2017 9:05 AM
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Any update yet? March 31, 2017 is fast approaching (smile). Thank you. v/r Jim

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office
U.S. Department of Homeland Security

(202) 447 (b)(6);(b) (office)
(202) 262 (7)(C) (cell)

"Liaison = Relationships + Communication"

IMPORTANT: This e-mail, including all attachments, constitutes Federal Government records and property that is intended only for the use of the individual or entity to which it is addressed. It may also contain information that is privileged, confidential, or otherwise protected from disclosure under applicable law. If the reader of this e-mail transmission is not the intended recipient or the employee or agent responsible for delivering the transmission to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this e-mail or its contents is strictly prohibited. If you have received this e-mail in error, please notify the sender by responding to the e-mail and then delete the e-mail immediately.

From: Crumpacker, Jim
Sent: Tuesday, February 21, 2017 7:27 PM
To: Balaban, Dorothy (b)(6);(b)(7)(C) @oig.dhs.gov>
Subject: Re: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Dottie:

Any word on this yet? I would like to get this resolved before the end of the next semi-annual reporting period (3/31/2017).

Also, does the IG anticipate that this report will come up during his congressional hearing about TSA in early March? If so, in what regard (i.e., the CCTV disagreement and/or the SSI marking issue)? Any insights appreciated. Thank you.

Jim

From: Crumpacker, Jim
Sent: Friday, February 17, 2017 09:26 AM Eastern Standard Time
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

?

From: Balaban, Dorothy
Sent: Wednesday, February 1, 2017 11:38 AM
To: Crumpacker, Jim (b)(6);(b)(7)(C) @HQ.DHS.GOV>
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

I'll chat with the IG after the hearing and let you know.

Dottie

From: Crumpacker, Jim
Sent: Wednesday, February 01, 2017 11:25:16 AM
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Dottie: FYI, I hope the hearing on “Empowering the Inspectors General” went well this morning. Unfortunately, I was not able to watch it due to competing priorities. BTW, I’ve still not heard anything from the IG concerning this non-concurrence. Know he has been extremely busy. Will continue to stand by. v/r Jim

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office
U.S. Department of Homeland Security

(202) 44 (b)(6);(b)(7)(C) (office)
(202) 26 (cell)

“Liaison = Relationships + Communication”

IMPORTANT: This e-mail, including all attachments, constitutes Federal Government records and property that is intended only for the use of the individual or entity to which it is addressed. It may also contain information that is privileged, confidential, or

IG Protests TSA's Edits of Audit Report

Inspector General John Roth of the Department of Homeland Security (DHS) has protested actions by Transportation Security Administration (TSA) officials requiring the deletion of material in a new Office of Inspector General (OIG) report. During their review of the OIG's *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport,* TSA officials classified sections of the report as Sensitive Security Information (SSI). By law, material labeled by TSA as SSI cannot be included in a public report.

Roth, who termed the TSA action an abuse of the SSI classification, reluctantly issued a redacted version to the public. But he has furnished a full, unedited report to congressional committees with oversight over TSA. The report contains findings and recommendations for improving the security of TSA systems at the airport.

"Over-classification is the enemy of good government. SSI markings should be used only to protect transportation security, rather than, as I fear occurred here, to allow government program officials to conceal negative information within a report," said Roth. "I believe – and the computer experts on my staff confirm – that this report should be released in its entirety in the public domain."

Roth dispatched a formal challenge memo to the TSA Administrator on November 19, 2014 and again on December 19, 2014. His memos also cited delays in TSA's review of the OIG report, which was issued to TSA officials in draft on July 22, 2014.

Roth noted that previous publicly released OIG reports had contained similar material and that the contents of the new report posed no threat to transportation security.

Citing multiple legal bases for full disclosure, Roth wrote that "our mission is to inform the public, Congress, and the DHS leadership about fraud, waste, and mismanagement in DHS programs and operations. Issuing full reports without edits is key to accomplishing that mission."

IG Protests TSA's Edits of Audit Report

Inspector General John Roth of the Department of Homeland Security (DHS) has protested actions by Transportation Security Administration (TSA) officials that resulted in the deletion of material in a new publicly released Office of Inspector General (OIG) report. During their review of the OIG's *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport,* TSA officials classified sections of the report as Sensitive Security Information (SSI). Such material cannot be included in a public report.

Roth, who termed the TSA action an unjustified abuse of the SSI classification, reluctantly issued a redacted version for public consumption. But he has furnished a full, unedited report to congressional committees with oversight over TSA. The report contains findings and recommendations for improving the security of TSA systems at the airport.

"SSI markings should not be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency," said Roth. "I believe that … this report should be released in its entirety in the public domain."

Roth aired his frustrations in December 16, 2014, memos to John Pistole, TSA Administrator, and Chip Fulgham, DHS Acting Under Secretary for Management. His memos also cited delays in TSA's review of the OIG report, which was issued to TSA officials in draft form on July 22, 2014. TSA officials finally notified the OIG on October 20, 2014, that, as a result of their sensitivity review, sections of the OIG report had been classified as SSI.

Roth noted that previous publicly released OIG reports had contained similar material and that the contents of the new report posed no threat to transportation security. He dispatched a formal challenge memo to Pistole on November 19, 2014. Pistole has not responded.

Citing multiple legal bases for full disclosure, Roth wrote that "our ability to issue reports that are transparent, without unduly restricting information, is key to accomplishing our mission."

IG Protests TSA's Edits of Audit Report

General John Roth has protested actions by the Transportation Security Administration to delete portions of an Office of Inspector General audit report by incorrectly classifying the material as Sensitive Security Information (SSI)

Information determined to be SSI cannot be included in a OIG report. Under protest, Roth has issued a redacted version for public consumption, but has furnished a full, unedited report to congressional committees with oversight over TSA.

Roth stated that "SSI markings should not be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency. I believe that … this report should be released in its entirety in the public domain.

Ross aired his frustrations in December 16, 2014, memos to John Pistole, TSA Administrator, and Chip Fulgham, the Department of Homeland Security Acting Under Secretary for Management, concerning the OIG report *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport.*

The report contains findings and recommendations for improving security controls over TSA servers, routers, switches, and telecommunications circuits at the airport.

Roth's memos also cited delays in TSA's review of the OIG report, which was issued to TSA officials in draft form on July 22, 2014. TSA officials finally notified the OIG on October 20, 2014, that, as a result of its sensitivity review, it had identified sections of the OIG report as SSI.

Roth protested that determination, noting that previous OIG reports had contained similar items and that the contents of OIG's report posed no threat to TSA's operations or to transportation security. Roth communicated his views to Pistole in a November 19, 2014, formal challenge memo. The TSA Administrator has yet to respond.

Citing multiple legal bases for full disclosure, Roth wrote that "our ability to issue reports that are transparent, without unduly restricting information, is key to accomplishing our mission."

Requester's Name: Shawn Musgrave

FOIA/PA NO.: 2015-087

4 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

3 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

From: Balaban, Dorothy
Sent: 17 Mar 2017 13:37:34 +0000
To: Roth, John
Subject: FW: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

FYI

From: Crumpacker, Jim
Sent: Friday, March 17, 2017 9:05 AM
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Any update yet? March 31, 2017 is fast approaching (smile). Thank you. v/r Jim

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office
U.S. Department of Homeland Security

(202) 447(b)(6);(b)(7)(C)office)
(202) 262 cell)

"Liaison = Relationships + Communication"

IMPORTANT: This e-mail, including all attachments, constitutes Federal Government records and property that is intended only for the use of the individual or entity to which it is addressed. It may also contain information that is privileged, confidential, or otherwise protected from disclosure under applicable law. If the reader of this e-mail transmission is not the intended recipient or the employee or agent responsible for delivering the transmission to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this e-mail or its contents is strictly prohibited. If you have received this e-mail in error, please notify the sender by responding to the e-mail and then delete the e-mail immediately.

From: Crumpacker, Jim
Sent: Tuesday, February 21, 2017 7:27 PM
To: Balaban, Dorothy <(b)(6);(b)(7)(C)@oig.dhs.gov>
Subject: Re: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Dottie:

Any word on this yet? I would like to get this resolved before the end of the next semi-annual reporting period (3/31/2017).

Also, does the IG anticipate that this report will come up during his congressional hearing about TSA in early March? If so, in what regard (i.e., the CCTV disagreement and/or the SSI marking issue)? Any insights appreciated. Thank you.

Jim

From: Crumpacker, Jim
Sent: Friday, February 17, 2017 09:26 AM Eastern Standard Time
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

?

From: Balaban, Dorothy
Sent: Wednesday, February 1, 2017 11:38 AM
To: Crumpacker, Jim (b)(6);(b)(7)(C) @HQ.DHS.GOV>
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

I'll chat with the IG after the hearing and let you know.

Dottie

From: Crumpacker, Jim
Sent: Wednesday, February 01, 2017 11:25:16 AM
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Dottie: FYI, I hope the hearing on "Empowering the Inspectors General" went well this morning. Unfortunately, I was not able to watch it due to competing priorities. BTW, I've still not heard anything from the IG concerning this non-concurrence. Know he has been extremely busy. Will continue to stand by. v/r Jim

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office
U.S. Department of Homeland Security

(202) 447 (b)(6);(b)(7)(C) (office)
(202) 262 (cell)

"Liaison = Relationships + Communication"

IMPORTANT: This e-mail, including all attachments, constitutes Federal Government records and property that is intended only for the use of the individual or entity to which it is addressed. It may also contain information that is privileged, confidential, or

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

5 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

From: Harsche, Richard
Sent: 20 Nov 2014 19:05:21 -0500
To: Balaban, Dorothy
Cc: Tsang, Chiu-Tong
Subject: Re: Anticipated SSI Program Schedules and SSI Review 14-0826

Dottie,
I noticed a small typo on page two. In the last sentence of the second bullet, the word "we" should be removed.
Rick

From: Balaban, Dorothy
Sent: Thursday, November 20, 2014 05:57 PM
To: Harsche, Richard
Cc: Tsang, Chiu-Tong
Subject: RE: Anticipated SSI Program Schedules and SSI Review 14-0826

Here's the memo to Pistole. Do you want me to send it to him, or do you want to send it to your counterpart?

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254 (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

From: Harsche, Richard
Sent: Thursday, November 20, 2014 2:03 PM
To: Balaban, Dorothy
Subject: FW: Anticipated SSI Program Schedules and SSI Review 14-0826

Dottie,
This information was provided by the Department for our SSI challenge memo. Please notice the email and cc information.
Rick

From: Eyl, Nancy
Sent: Thursday, November 20, 2014 1:11 PM
To (b)(6)
Cc: Harsche, Richard; Mobbs, Michael
Subject: Re: Anticipated SSI Program Schedules and SSI Review 14-0826

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

2 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

From: Harsche, Richard
Sent: 20 Nov 2014 18:24:31 -0500
To: Balaban, Dorothy;Tsang, Chiu-Tong
Subject: RE: Anticipated SSI Program Schedules and SSI Review 14-0826

Agree. Thanks, Dottie.
Rick

From: Balaban, Dorothy
Sent: Thursday, November 20, 2014 6:05 PM
To: Tsang, Chiu-Tong; Harsche, Richard
Subject: RE: Anticipated SSI Program Schedules and SSI Review 14-0826

Will do. No problem.

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254 (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

From: Tsang, Chiu-Tong
Sent: Thursday, November 20, 2014 6:05 PM
To: Balaban, Dorothy; Harsche, Richard
Subject: Re: Anticipated SSI Program Schedules and SSI Review 14-0826

Dottie,

Since the memo is going to the TSA Director, maybe it's appropriate if you can send it out, if you don't mind?

Thanks.

Tom

Tom Tsang
Director, Information Security Audit Division
DHS OIG
Office-202-254 (b)(6);(b)(7)(C)
BlackBerry-20
Sent from my BlackBerry Wireless Handheld

From: Balaban, Dorothy
Sent: Thursday, November 20, 2014 05:57 PM
To: Harsche, Richard
Cc: Tsang, Chiu-Tong
Subject: RE: Anticipated SSI Program Schedules and SSI Review 14-0826

Here's the memo to Pistole. Do you want me to send it to him, or do you want to send it to your counterpart?

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-254 (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

From: Harsche, Richard
Sent: Thursday, November 20, 2014 2:03 PM
To: Balaban, Dorothy
Subject: FW: Anticipated SSI Program Schedules and SSI Review 14-0826

Dottie,
This information was provided by the Department for our SSI challenge memo. Please notice the email and cc information.
Rick

From: Eyl, Nancy
Sent: Thursday, November 20, 2014 1:11 PM
To (b)(6)
Cc: Harsche, Richard; Mobbs, Michael
Subject: Re: Anticipated SSI Program Schedules and SSI Review 14-0826

(b)(6)

Thank you for writing. I am forwarding your message to our AIG for IT audits. Rick Harsche has a better handle on this than I do.

Best
Nancy

Requester's Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

2 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

From: Tsang, Chiu-Tong
Sent: 20 Nov 2014 18:04:49 -0500
To: Balaban, Dorothy;Harsche, Richard
Subject: Re: Anticipated SSI Program Schedules and SSI Review 14-0826

Dottie,

Since the memo is going to the TSA Director, maybe it's appropriate if you can send it out, if you don't mind?

Thanks.

Tom

Tom Tsang
Director, Information Security Audit Division
DHS OIG
Office-202-25 (b)(6);(b)(7)(C)
BlackBerry-20
Sent from my BlackBerry Wireless Handheld

From: Balaban, Dorothy
Sent: Thursday, November 20, 2014 05:57 PM
To: Harsche, Richard
Cc: Tsang, Chiu-Tong
Subject: RE: Anticipated SSI Program Schedules and SSI Review 14-0826

Here's the memo to Pistole. Do you want me to send it to him, or do you want to send it to your counterpart?

Dottie

Dottie Balaban
Special Assistant to the Inspector General
Office of Inspector General
202-25 (b)(6);(b)(7)(C)

Notary Public for the District of Columbia

From: Harsche, Richard
Sent: Thursday, November 20, 2014 2:03 PM
To: Balaban, Dorothy
Subject: FW: Anticipated SSI Program Schedules and SSI Review 14-0826

Requester’s Name: Shawn Musgrave
FOIA/PA NO.: 2015-087

1 PAGES OF

DUPLICATES (DUP)
HELD IN THE FILE

From: Crumpacker, Jim
Sent: 17 Mar 2017 09:04:42 -0400
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Any update yet? March 31, 2017 is fast approaching (smile). Thank you. v/r Jim

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office
U.S. Department of Homeland Security

(202) 447-(b)(6);(b)(7)(C) office)
(202) 262- cell)

"Liaison = Relationships + Communication"

IMPORTANT: This e-mail, including all attachments, constitutes Federal Government records and property that is intended only for the use of the individual or entity to which it is addressed. It may also contain information that is privileged, confidential, or otherwise protected from disclosure under applicable law. If the reader of this e-mail transmission is not the intended recipient or the employee or agent responsible for delivering the transmission to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this e-mail or its contents is strictly prohibited. If you have received this e-mail in error, please notify the sender by responding to the e-mail and then delete the e-mail immediately.

From: Crumpacker, Jim
Sent: Tuesday, February 21, 2017 7:27 PM
To: Balaban, Dorothy <Dorothy.Balaban@oig.dhs.gov>
Subject: Re: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Dottie:

Any word on this yet? I would like to get this resolved before the end of the next semi-annual reporting period (3/31/2017).

Also, does the IG anticipate that this report will come up during his congressional hearing about TSA in early March? If so, in what regard (i.e., the CCTV disagreement and/or the SSI marking issue)? Any insights appreciated. Thank you.

Jim

From: Crumpacker, Jim
Sent: Friday, February 17, 2017 09:26 AM Eastern Standard Time
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

?

From: Balaban, Dorothy
Sent: Wednesday, February 1, 2017 11:38 AM
To: Crumpacker, Jim (b)(6);(b)(7)(C) @HQ.DHS.GOV>
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

I'll chat with the IG after the hearing and let you know.

Dottie

From: Crumpacker, Jim
Sent: Wednesday, February 01, 2017 11:25:16 AM
To: Balaban, Dorothy
Subject: RE: Audit of Security Controls for Information Technology Systems at John F Kennedy International Airport" (OIG-15-18)

Dottie: FYI, I hope the hearing on "Empowering the Inspectors General" went well this morning. Unfortunately, I was not able to watch it due to competing priorities. BTW, I've still not heard anything from the IG concerning this non-concurrence. Know he has been extremely busy. Will continue to stand by. v/r Jim

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office
U.S. Department of Homeland Security

(202) 447 (b)(6);(b)(7)(C) (office)
(202) 262 (cell)

"Liaison = Relationships + Communication"

IMPORTANT: This e-mail, including all attachments, constitutes Federal Government records and property that is intended only for the use of the individual or entity to which it is addressed. It may also contain information that is privileged, confidential, or otherwise protected from disclosure under applicable law. If the reader of this e-mail transmission is not the intended recipient or the employee or agent responsible for delivering the transmission to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this e-mail or its contents is strictly prohibited. If you have received this e-mail in error, please notify the sender by responding to the e-mail and then delete the e-mail immediately.

From: Crumpacker, Jim
Sent: Tuesday, January 24, 2017 4:10 PM
To: Balaban, Dorothy (b)(6);(b)(7)(C) @oig.dhs.gov) (b)(6);(b)(7)(C) @oig.dhs.gov>

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

DEC 16 2014

MEMORANDUM FOR: The Honorable Chip Fulghum
Acting Under Secretary for Management

FROM: John Roth John Roth
Inspector General

SUBJECT: *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport*

Attached for your information is our final report, *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport.* This report contains findings and recommendations for improving security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS information technology infrastructure at this airport.

We provided a draft of this report on July 22, 2014, for review. On October 20, 2014, the Departmental GAO-OIG Liaison Office finally conveyed the TSA Sensitive Security Information (SSI) Program Office's response to our request for a sensitivity review by marking several passages in the report as SSI. I disagree with this determination. On November 19, 2014, I sent a formal challenge memo to TSA Administrator John Pistole and copied SSI Program Chief Doug Blair, expressing my disagreement. My challenge is in accordance with procedures outlined in DHS Management Directive MD11056.1. Under this directive, a formal challenge may be submitted, in writing, to the person who made the SSI markings or to the SSI Office.

To date, I have not yet received a response from TSA. I challenged TSA's determination based on the following:

- First, the same or similar information as that marked as SSI in the current draft report was disclosed to the public in previously released DHS OIG and GAO reports. The Department reviewed and approved the content of these previously released reports and did not determine at the time that the information was SSI. See, e.g., *Audit of Security Controls for DHS Information Technology Systems*

at Dallas/Fort Worth International Airport, OIG-14-132 (September 2014).

- Second, even if past reports had not released similar information, its release in this report would not be detrimental to transportation security. For example, the language marked SSI reveals generic vulnerabilities that are common to virtually all systems. In addition, the descriptions of the vulnerabilities are not specific enough to be detrimental. We have published similar findings in reports concerning other DHS components with no detrimental impact. See, e.g., *Implementation Status of EINSTEIN 3 Accelerated*, OIG-14-52 (March 2014).

- Lastly, although the SSI Office marked information in the TSA and CBP Patch Management sections of the draft report as SSI, the SSI Program Office did not mark the same information in another section of the very same report as SSI. Specifically, the ICE section of the draft report includes the same table and wording regarding scanning vulnerabilities as in the TSA and CBP sections. As such, the SSI determination appears to be inconsistently applied.

For these reasons, I have requested that the TSA Administrator reconsider and remove its SSI markings from our draft report. These markings impede the effectiveness and transparency of our office. Per DHS MD 11056.1, section VI.A.3, SSI markings should not be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency. I believe that based on the reasons outlined above, this report should be released in its entirety in the public domain.

The Inspector General Act requires the OIG to conduct audits and investigations that promote the economy, efficiency, and effectiveness of DHS programs and operations, and to keep the Secretary and the Congress fully and timely informed. *The Inspector General Act* also requires the OIG to post its audit reports, or portions thereof, on its website so that the public may easily access the information. Our ability to issue reports that are transparent, without unduly restricting information, is key to accomplishing our mission.

In 2006, Congress, concerned about delays in appeals of this nature, directed the Department to revise MD 11056.1 to require TSA to ensure a timely SSI review of public requests for release of information. Given the

clear requirement in MD 11056.1, for timely SSI reviews in response to requests from the public, we hoped that TSA would approach an SSI appeal from a fellow component with similar diligence, especially since TSA is aware of our deadlines. We are disappointed. Now, to meet our reporting deadline, we are compelled to publish a redacted report with SSI markings we believe are incorrect since we still have not received a timely response to our SSI challenge memorandum.

Congress, when it passed the *Reducing Over-Classification Act* in 2010, found that overclassification "interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information." The Act directed DHS to take steps to guard against over-classification.

Consistent with our responsibilities under the *Inspector General Act*, we will provide unredacted copies of our report to appropriate Congressional Committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted report on our website for public dissemination.

I appreciate your attention to this matter. Should you have any questions, please call me, or your staff may contact Sondra McCauley, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4041.

Attachment

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

NOV 19 2014

MEMORANDUM FOR: The Honorable John Pistole
Administrator
Transportation Security Administration

FROM: John Roth John Roth
Inspector General

SUBJECT: Office of Inspector General's Challenge to Sensitive Security Information Office's Request to Mark OIG report: *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport* as SSI
OIG *Project No: 14-082-ITA-DHS*

The Inspector General Act requires the Office of Inspector General (OIG) to conduct audits and investigations that promote the economy, efficiency, and effectiveness of DHS programs and operations, and to inform the Secretary, Congress, and the public about any problems and deficiencies we identify. Our ability to issue reports to the public that are transparent, without unduly restricting information, is key to accomplishing our mission.

I am concerned that the Department's review and response to our draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport,* indicated that several statements within the report were determined to be Sensitive Security Information (SSI). I disagree with this determination and I am submitting this formal challenge according to procedures outlined in DHS Management Directive MD 11056.1, Sensitive Security Information. Under DHS MD 11056.1.F.2, a formal challenge may be submitted, in writing, to the person who made the SSI markings or to the SSI Office.

We issued the draft report, *Technical Security Evaluation of DHS Activities at JFK International Airport,* to the Department on July 22, 2014. On August 6, 2014, a SSI Senior Program Analyst, provided a response and marked as SSI several passages in this report. See Attachment A for a copy of this draft report with the suggested SSI content highlighted. I recognize the SSI Office's process to identify and safeguard SSI information. However, I believe the information in our draft report was

improperly marked as SSI and I am challenging this determination based on the following:

First, the same or similar information as that marked SSI in the current draft report was disclosed to the public in previously released DHS OIG and GAO reports. The Department reviewed and approved the content of these previously released reports and did not determine at that time that the information was SSI. For example:

- On page 5 of our draft report, we discuss physical security issues in TSA's space at JFK airport. The SSI Office marked this information as SSI based on 49 C.F.R. § 1520.5(b) (5). I challenge this request. In GAO audit report *General Aviation: Security Assessments at Selected Airports*, GAO-11-298 dated May 2011, GAO published similar information. Specifically, the GAO report discusses and reports the security measures and potential vulnerabilities at selected airports. (page 7, Attachment B)
- Also, on page 5 of our draft report, we display a picture of TSA equipment in a corridor accessible by unsecured double doors to public area prior to TSA terminal security checkpoint. The SSI Office marked this picture SSI. I challenge this request. This is a picture of IT equipment similar to the IT equipment pictured in figures 4, 5, and 6 of our draft report, yet the SSI Office did not mark those figures SSI. This item shows an example of a TSA equipment cabinet that is in an area accessible to non TSA staff and the public. This risk can be controlled and eliminated by TSA simply securing the terminal corridor from unauthorized access. In addition, our report did not provide the specific location of this cabinet.
- On pages 14 and 21 of our draft report, the SSI office marked one sentence on each page as SSI information. These sentences are located in the TSA (page 14) and CBP (page 21) Patch Management Sections of our report. I challenge this request. Similar or the same wording was used in our last two publically released technical security airport reviews at Dallas Ft. Worth (*Audit of Security Controls for DHS Information Technology Systems at Dallas/Ft. Worth International Airport*, OIG-14-132) and Atlanta's Hartsfield (*Technical Security Evaluation of DHS Activities at Hartsfield Jackson Atlanta International Airport*, OIG-13-104) airports. (pages 10, 18, and 25 in Attachment C and pages 10, 20, and 31 in Attachment D)

- Also on pages 14 and 21 of our draft report, the SSI office marked information in the tables in the TSA and CBP Patch Management sections of the report as SSI information. I challenge this request. Similar content in the same table format was reported in our last two publically released DHS OIG audit reports on Dallas/Ft. Worth, OIG-14-132, and Atlanta Hartsfield airports OIG-13-104. (pages 10, 18, and 25 in Attachment C and pages 10, 20, and 31 in Attachment D)

Second, although the SSI Office marked information in the TSA and CBP Patch Management sections of the draft report as SSI, the SSI Office did not mark the same information in the ICE section of the same report as SSI. Specifically, the ICE section of the draft report includes the same table and wording regarding scanning vulnerabilities that is in the TSA and CBP sections. However, the SSI office did not mark the ICE information as SSI. The SSI determination appears to be inconsistently applied.

Further, even if past reports had not released similar information, I still do not believe its release in this report would be detrimental to transportation security. For example, the language marked SSI reveals generic vulnerabilities that are common to virtually all systems. In addition, the descriptions of the vulnerabilities are not specific enough to be detrimental.

For these reasons, I am requesting that you reconsider and remove your SSI markings from our draft report. These markings impede the effectiveness and transparency of our office. I feel that based on the reasons I have outlined above, our OIG report, *Technical Security Evaluation of DHS Activities at JFK International Airport,* should be released in its entirety in the public Domain.

I appreciate your attention to this matter. Please feel free to contact me with any questions.

cc: Jim Crumpacker, Director, DHS GAO/OIG Liaison Office
Shelly Peterson, Audit Liaison for the Chief Information Officer
Susan Perkins, TSA, Audit Liaison
Tamara Lilly, DHS CISO, Audit Liaison
John Buckley, CBP, CISO
Judy Wright, CBP, Audit Liaison
Tom DeBiase, ICE, Acting CISO

Joanna Perkins, ICE, Audit Liaison
Jill Vaughan, TSA, CISO
Thomas Feltrin, TSA, Audit Liaison
Doug Blair, SSI Program Chief
Rob Metzler, Senior Analyst

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

DEC 1 6 2014

MEMORANDUM FOR: The Honorable John Pistole
Administrator
Transportation Security Administration

FROM: John Roth
Inspector General

SUBJECT: Follow up to my Challenge Memo to the SSI Markings to draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport-Sensitive Security Information*

I am writing to follow up on the memo I sent you on November 19, 2014, regarding my challenge to Sensitive Security Information (SSI) markings to our draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport.* We are preparing to issue this report as final. However, I am concerned that I have not heard back from you regarding my request to remove the SSI markings from our report so that we may issue it in its entirety in the public domain.

In response to a law passed by the Congress in 2006, the Department revised DHS Management Directive (MD) 11056.1, to require TSA to ensure a timely SSI review of public requests for release of information. Given MD 11056.1, section V.B.7's requirement for timely SSI reviews in response to requests from the public, we hoped that TSA would approach our SSI appeal from a fellow component with similar diligence, especially since TSA is aware of our deadlines. We are disappointed.

In its October 20, 2014, response to our draft report, the Department indicated that several statements within the report were determined to be SSI. I disagree with the markings and submitted my challenge to you in accordance with guidance provided under MD 11056.1.

I again request that you reconsider and remove the SSI markings from our draft report. I recognize the SSI Office's process to identify and safeguard SSI information. However, I believe that improperly marking information in our draft report as SSI impedes our ability to issue reports to the public that are transparent, without unduly restricting information, which is key to accomplishing our mission. Per DHS MD

11056.1, VI.A.3, SSI markings should not be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency.

This report has languished for months because of TSA's sensitivity review. Absent a decision from you, we will be forced to publish a redacted report to meet our timeliness requirements. The report will contain our objections to the redactions. Consistent with our responsibilities under the *Inspector General Act,* we will provide unredacted copies of our report to Congressional Committees with oversight and appropriations responsibility for the Department of Homeland Security.

I appreciate your personal attention to this matter and I await your response. Should you have any questions, please call me.

Attachment

Requester's Name: Shawn Musgrave

2015-087

1 PAGE(S) OF DOCUMENT(S)

WITHHELD IN FULL (WIF)

EXEMPTIONS CITED

(b)(5)

Document ID: 0.7.368.5030

From: Roth, John </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6);(b)(7)(C)oig.dhs.gov747>
To: Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6);(b)(7)(C)dhs.gov>; McCauley, Sondra </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6);(b)(7)(C)oig.dhs.govdab>
Cc: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6);(b)(7)(C)dhs.gov>; Eyl, Nancy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6);(b)(7)(C)dhs.gov>
Bcc:
Subject: JFK and SSI
Date: Thu Dec 04 2014 10:19:15 EST
Attachments: @

See section 525 &#8211; SSI appeals must be reviewed in &#8220;a timely manner,&#8221; and congress directed the relevant MD to be amended to reflect that. Assuming I have the most recent version of the MD, that hasn&#8217;t been done. That should also be pointed out in the letter as well. We should also point out that the SSI statute is not to be used merely to hide embarrassing information.

From: Harsche, Richard
Sent: Thursday, December 04, 2014 9:45 AM
To: Roth, John; McCauley, Sondra
Cc: Balaban, Dorothy
Subject: RE: would you have a few minutes before 11 am to discuss JFK? Thanks.

10 will work for both of us.

Rick

From: Roth, John
Sent: Thursday, December 04, 2014 9:30 AM
To: Harsche, Richard; McCauley, Sondra
Cc: Balaban, Dorothy
Subject: would you have a few minutes before 11 am to discuss JFK? Thanks.

Document ID: 0.7.368.5030-000001

null
Last Modified: Thu Dec 04 10:19:15 EST 2014

Document ID: 0.7.368.5033-000001

null
Last Modified: Fri Jan 09 13:59:44 EST 2015

Document ID: 0.7.368.5025

From: Roth, John </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)oig.dhs.gov747>
To: Paulson, Erica </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn(b)(6)dhs.gov>
Cc: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
Bcc:
Subject: RE: JFK Press Release
Date: Wed Jan 21 2015 10:05:46 EST
Attachments: @

Of course. Hillburg thought that ordinary people wouldn&#8217;t understand what a redaction was.

From: Paulson, Erica
Sent: Wednesday, January 21, 2015 10:02 AM
To: Roth, John
Cc: Balaban, Dorothy
Subject: RE: JFK Press Release

I have one suggested word change to your quote in the last sentence &#8211; changing &#8220; edits&#8221; to &#8220;redactions&#8221;. Is that okay?

Citing multiple legal bases for full disclosure, Roth wrote that &#8220;our mission is to inform the public, Congress, and the DHS leadership about fraud, waste, and mismanagement in DHS programs and operations. Issuing full reports without edits redactions is key to accomplishing that mission.&#8221;

From: Roth, John
Sent: Wednesday, January 21, 2015 8:48 AM
To: Paulson, Erica
Cc: Balaban, Dorothy
Subject: RE: JFK Press Release

Attached. Thanks. Give it a good read before launching.

From: Paulson, Erica
Sent: Tuesday, January 20, 2015 5:59 PM
To: Roth, John
Cc: Balaban, Dorothy
Subject:

Document ID: 0.7.368.5025-000001

null
Last Modified: Wed Jan 21 10:05:46 EST 2015

Document ID: 0.7.368.5040

From: Huiswoud, Sharon
</o=dhs-oig/ou=headquarters/cn=recipients/cn=headquarters-1/cn=
information technology/cn=information systems &
architectures/cn=users/cn= (b)(6)
To: Balaban, Dorothy </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn= (b)(6) dhs.gov>
Cc:
Bcc:
Subject: FW: Audit Draft Report Response: Technical Security Evaluation of DHS Activities at JFK Airport, OIG-14-082-ITA-MGMT
Date: Wed Aug 27 2014 18:42:26 EDT
Attachments:

Hi Dottie-

I see the OCIO sent a request to the IG for an extension to respond to my report. Since Rick is out this week I would say that we would prefer to have the response sooner so that we can make the 9/30 cut off, but of course we understand the circumstances. Of course I know that the final say is up to Mr. Roth. :) Have a good evening....

Sharon L. Huiswoud
Director
Information Systems Division
Office of IT Audits
Department of Homeland Security
Office of Inspector General
office: 202-254 (b)(6)
cell: 202-497 (b)(6)

-----Original Message-----
From: (b)(6)
Sent: Wednesday, August 27, 2014 5:11 PM
To: Roth, John
Cc: (b)(6) Huiswoud, Sharon
Subject: Audit Draft Report Response: Technical Security Evaluation of DHS Activities at JFK Airport, OIG-14-082-ITA-MGMT

Mr. Roth,

OCIO would like to request an extension to provide the draft response letter and technical comments regarding the O

Document ID: 0.7.368.5041

From: Huiswoud, Sharon </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6).dhs.gov>
To: Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn(b)(6)dhs.gov>; Huiswoud, Sharon </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn(b)(6)dhs.gov>
Cc: Grady, Sharell </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn(b)(6)dhs.gov>; Eyl, Nancy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn(b)(6)dhs.gov>; Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
Bcc:
Subject: Re: Update on TSA SSI Process for JFK
Date: Thu Nov 06 2014 17:23:58 EST
Attachments:

Ok...will do, thanks

Sharon Huiswoud
Director, IT Audits
DHS OIG
202-254(b)(6)

From: Harsche, Richard
Sent: Thursday, November 06, 2014 04:06 PM
To: Huiswoud, Sharon
Cc: Grady, Sharell; Eyl, Nancy; Balaban, Dorothy
Subject: Update on TSA SSI Process for JFK

Sharon,

I gave the IG the binder that you provided me this afternoon. After a conversation, Mr. Roth stated that he would like to take a dual track on this SSI issue. Specifically, he would like your team and Nancy to:

1) Put together a formal package/memo to challenge the SSI (legal opinion option #1 in the binder), and

2) Issue the report as SSI with a memo stating that we are issuing the report as SSI, but do not agree with TSA&#8217;s determination. We will also state in the memo that we are formally challenging the SSI designation. (legal opinion option #3 in the binder)

I will not be in the office tomorrow, Friday, but let&#8217;s get started drafting these memos and pus

Document ID: 0.7.368.5042

From: Harsche, Richard </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
To: Huiswoud, Sharon </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn= (b)(6) dhs.gov>
Cc: Grady, Sharell </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>;
Eyl, Nancy </o=dhs/ou=exchange administrative group
(fydibohf23spdlt)/cn=recipients/cn= (b)(6) dhs.gov>; Balaban,
Dorothy </o=dhs/ou=exchange administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
Bcc:
Subject: Update on TSA SSI Process for JFK
Date: Thu Nov 06 2014 16:06:13 EST
Attachments:

Sharon,

I gave the IG the binder that you provided me this afternoon. After a conversation, Mr. Roth stated that he would like to take a dual track on this SSI issue. Specifically, he would like your team and Nancy to:

1) Put together a formal package/memo to challenge the SSI (legal opinion option #1 in the binder), and

2) Issue the report as SSI with a memo stating that we are issuing the report as SSI, but do not agree with TSA&#8217;s determination. We will also state in the memo that we are formally challenging the SSI designation. (legal opinion option #3 in the binder)

I will not be in the office tomorrow, Friday, but let&#8217;s get started drafting these memos and push to get the report up to the front office as soon as possible. We can talk more on Monday concerning the progress.

Lastly, the IG does not think that it will be necessary to meet on Monday, as we now have a game plan to move this forward.

Thanks,

Rick

Richard Harsche

Document ID: 0.7.368.5032-000001

null
Last Modified: Tue Feb 10 10:08:53 EST 2015

Document ID: 0.7.368.5015

From: Paulson, Erica </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn= (b)(6) dhs.gov>
To: Roth, John </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) .oig.dhs.gov747>
Cc: DHS-OIG Office of Public Affairs </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=dhs-oig.officepublicaffairs.oig.dhs.govd04>; Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>; McCauley, Sondra </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn= (b)(6) .oig.dhs.govdab>
Bcc:
Subject: Washington Post on TSA Redactions
Date: Sat Jan 24 2015 11:13:21 EST
Attachments: @

Josh Hicks picked up the story and did a nice little blurb:

http://www.washingtonpost.com/blogs/federal-eye/wp/2015/01/23/inspector-general-blasts-tsa-over-redactions-for-jfk-airport-audit/

Federal Eye <http://www.washingtonpost.com/blogs/federal-eye/>

Inspector general rips TSA over redaction of JFK airport audit

The Transportation Security Administration abused its authority to classify information as too sensitive for release when it blocked sections of a recent audit report <http://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-18_Jan14.pdf> from being published, according to the agency&#8217;s independent watchdog.

Department of Homeland Security Inspector General John Roth protested TSA&#8217;s actions on Friday, saying in a statement <http://www.oig.dhs.gov/assets/pr/2015/oigpr_012315.pdf> that he suspects that agency officials wanted to &#8220;conceal negative information.&#8221;

Roth&#8217;s complaint relates to his office&#8217;s recent report on shortcomings with TSA&#8217;s computer sec

Document ID: 0.7.368.5015-000001

null
Last Modified: Sat Jan 24 11:13:21 EST 2015

Document ID: 0.7.368.5027-000001

null
Last Modified: Fri Jan 09 14:14:17 EST 2015

Document ID: 0.7.368.5028

From: Huiswoud, Sharon </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cr (b)(6) dhs.gov>
To: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn= (b)(6) dhs.gov>
Cc:
Bcc:
Subject: FW: Anticipated SSI Program Schedules and SSI Review 14-0826
Date: Fri Jan 16 2015 13:37:54 EST
Attachments:

Hi Dottie

Below is the information that show Robert Metzler was communicating with our counsel.

Sharon L. Huiswoud

Director

Information Systems Division

Office of IT Audits

Department of Homeland Security

Office of Inspector General

office: 202-254 (b)(6)

cell: 202-497- (b)(6)

From: Eyl, Nancy
Sent: Thursday, November 20, 2014 1:11 PM
T (b)(6)
Cc: Harsche, Richard; Mobbs, Michael
Subject: Re: Anticipated SSI Program Schedules and SSI Review 14-0826

(b)(6)

Thank you for writing. I am forwarding your message to our AIG for IT audits. Rick Harsche has a better handle on this than I do.

Best
Nancy

Document ID: 0.7.368.5016

From: Huiswoud, Sharon </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn(b)(6)dhs.gov>
To: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
Cc:
Bcc:
Subject: FW: Audit Draft Report Response: Technical Security Evaluation of DHS Activities at JFK Airport, OIG-14-082-ITA-MGMT
Date: Fri Sep 12 2014 11:00:47 EDT
Attachments:

Hi Dottie-

Just some FYI...Mr. Roth granted the OCIO an extension to respond to our draft report on JFK(below). We just talked to the OCIO audit liaison Shelly Peterson and she said that they will need another extension, the components have some areas that they would like redacted and TSA says that there are SSI issues that will need to be redacted as well. I talked to Rick Harsche and told him that I asked the DHS CIO Luke McCormack to send over another request to Mr. Roth with this information in it and he will let them know if he approves the request. Thanks,

Sharon L. Huiswoud
Director
Information Systems Division
Office of IT Audits
Department of Homeland Security
Office of Inspector General
office: 202-25(b)(6)
cell: 202-497-
-----Original Message-----
From: Roth, John
Sent: Thursday, August 28, 2014 7:55 AM
To: Whitelaw, Barbara
Cc: (b)(6) Huiswoud, Sharon
Subject: RE: Audit Draft Report Respons

Document ID: 0.7.368.5037

From: McCauley, Sondra </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)oig.dhs.govd ab>
To: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=(b)(6)dhs.gov>
Cc:
Bcc:
Subject: JFK report redaction issue
Date: Thu Jan 15 2015 10:22:22 EST
Attachments:

Dottie:

I would like Sharon Huiswoud to attend the meeting with the IG at 3 pm on the JFK meeting. She is the responsible Director and the SME on this issue, so I would like to have her involved firsthand in the discussion. Is that okay?

Sondra McCauley

Assistant Inspector General for Information Technology Audits

Department of Homeland Security

Office of Inspector General

Work: 202-254(b)(6)

Cell: 202-425(b)(6)

(b)(6)@oig.dhs.gov

Document ID: 0.7.368.5038

From: Morales, Arlen </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn= (b)(6) dhs.gov>
To: Roth, John </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/c (b)(6) oig.dhs.gov747>
Cc: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn= (b)(6) dhs.gov>; Hillburg, William </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn= (b)(6) oig.dhs.gov 085>
Bcc:
Subject: FW: JFK presser(2)
Date: Tue Dec 23 2014 09:08:52 EST
Attachments:

Good Morning Mr. Roth,

Hope this email finds you well.

Should we edit the JFK presser since Mr. Pistole will retire?

Thank you.

IG Protests TSA&#8217;s Edits of Audit Report

Inspector General John Roth of the Department of Homeland Security (DHS) has protested actions by Transportation Security Administration (TSA) officials requiring the deletion of material in a new Office of Inspector General (OIG) report. During their review of the OIG&#8217;s Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport, TSA officials classified sections of the report as Sensitive Security Information (SSI). By law, material labeled by TSA as SSI cannot be included in a public report.

Roth, who termed the TSA action an abuse of the SSI classification, reluctantly issued a redacted version for public consumption. But he has furnished a full, unedited report to congressional committee

Document ID: 0.7.368.5008

From: Grady, Sharell </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
To: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn(b)(6)dhs.gov>
Cc: Huiswoud, Sharon </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>; Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn(b)(6)dhs.gov>
Bcc:
Subject: FW: Memo on Formal Request to Challenge SSI Office.docx
Date: Thu Nov 13 2014 15:09:19 EST
Attachments: @

Attached is the memo for our formal request and supporting documentation. Our draft report is secured: Password to follow.

Sharell Grady
Audit Manager
DHS/OIG/Office of IT Audit
Information Systems Division
Office: 202 254(b)(6)
Blackberry: 202 36(b)(6)

Document ID: 0.7.368.5008-000001

null
Last Modified: Thu Nov 13 15:09:19 EST 2014

Document ID: 0.7.368.5009

From: Roth, John </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cr (b)(6) ig.dhs.gov747>
To: Hillburg, William </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cr (b)(6) oig.dhs.gov 085>; Paulson, Erica </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn= (b)(6) dhs.gov>
Cc: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
Bcc:
Subject: FW: JFK Memos
Date: Wed Dec 17 2014 07:52:14 EST
Attachments: @

FYI. Bill, I will want a press release on the JFK report, focusing more on TSA&#8217;s attempt to hide information and less on the substance of the report. Dottie will get you a copy.

From: Balaban, Dorothy
Sent: Tuesday, December 16, 2014 1:56 PM
To: Roth, John
Subject: JFK Memos

Here are the two signed memos.

Dottie

Dottie Balaban

Special Assistant to the Inspector General

Office of Inspector General

202-25 (b)(6)

Notary Public for the District of Columbia

Document ID: 0.7.368.5009-000001

null
Last Modified: Wed Dec 17 07:52:14 EST 2014

Document ID: 0.7.368.5031

From: Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
To: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn= (b)(6) dhs.gov>
Cc:
Bcc:
Subject: JFK Report
Date: Wed Dec 24 2014 08:06:18 EST
Attachments:

Dottie,

I understand that Sharon Huiswoud has resolved the SSI marking issues with the JFK report and has routed it back to you. Please let me know if you have any other concerns or questions.

Have a great holiday!

Rick

From: Huiswoud, Sharon
Sent: Wednesday, December 24, 2014 7:25 AM
To: Harsche, Richard
Subject: RE: Hey...

Yes, I spoke with Nancy and Dottie yesterday. There were two places in the SSI version where there were highlights but these areas were not blacked out in the redacted version. Sharell just fixed them and put the report back out there to Dottie. Once the IG approves, Sharell will remove the highlights from the SSI version and the report will be ready to issue.

Sharon L. Huiswoud

Director

Information Systems Division

Office of IT Audits

Department of Homeland Security

Office of Inspector General

office: 202-25 (b)(6)

cell: 202-497 (b)(6)

From: Harsche, Richard
Sent: Wednesday, December 24, 2014 7:22 AM

Document ID: 0.7.368.5029

From: McCauley, Sondra </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) oig.dhs.govd
ab>
To: Roth, John </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) oig.dhs.gov747>;
Harsche, Richard </o=dhs/ou=exchange administrative group
(fydibohf23spdlt)/cn=recipients/cn= (b)(6) dhs.gov>
Cc: Balaban, Dorothy </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>;
Eyl, Nancy </o=dhs/ou=exchange administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>;
Huiswoud, Sharon </o=dhs/ou=exchange administrative group
(fydibohf23spdlt)/cn=recipients/cn= (b)(6) dhs.gov>
Bcc:
Subject: RE: JFK and SSI
Date: Thu Dec 04 2014 10:28:04 EST
Attachments:

John:

Thank you. We will follow-up to ensure this is the latest guidance.

Sondra

From: Roth, John
Sent: Thursday, December 04, 2014 10:19 AM
To: Harsche, Richard; McCauley, Sondra
Cc: Balaban, Dorothy; Eyl, Nancy
Subject: JFK and SSI

See section 525 &#8211; SSI appeals must be reviewed in &#8220;a timely manner,&#8221; and congress directed the relevant MD to be amended to reflect that. Assuming I have the most recent version of the MD, that hasn&#8217;t been done. That should also be pointed out in the letter as well. We should also point out that the SSI statute is not to be used merely to hide embarrassing information.

From: Harsche, Richard
Sent: Thursday, December 04, 2014 9:45 AM
To: Roth, John; McCauley, Sondra
Cc: Balaban, Dorothy

Subject: RE: would you have a few minutes before 11 am to discuss JFK? Thanks.

10 will work for both of us.

Rick

From: Roth, John
Sent: Thursday, December 04, 2014 9:30 AM
To: Harsche, Richard; McCau

Document ID: 0.7.368.5035

From: Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
To: Roth, John </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/c (b)(6) oig.dhs.gov747>
Cc: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
Bcc:
Subject: RE: memo to Doug Blair re JFK SSI
Date: Fri Nov 14 2014 11:29:16 EST
Attachments:

Sir,

I checked with the team and they advised that the memo does not contain SSI. Therefore, there is no need to mark it as such. We also believe that the memo is going to the appropriate person/level. We could/should copy Mr. Pistole. (I understand that he is retiring from TSA on December 31st, but this should not be an issue.) We probably should request a timeframe for a response and suggest 3 business days. Lastly, I agree that we should be explicit about our next steps and adjust the memo as necessary, assuming that we do not receive a timely response.

Rick

From: Roth, John
Sent: Friday, November 14, 2014 10:59 AM
To: Harsche, Richard
Cc: Balaban, Dorothy
Subject: memo to Doug Blair re JFK SSI

Nice memo. I signed it and didn&#8217;t have any edits.

After I signed it, some things came to mind, though: 1) is there any potential PII within the memo? If so, do we need to appropriately mark the memo?; 2) who should this be addressed to? Pistole is

Document ID: 0.7.368.5020

From: Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
To: Roth, John </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)oig.dhs.gov747>
Cc: Eyl, Nancy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>; Huiswoud, Sharon </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cr(b)(6)dhs.gov>; Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
Bcc:
Subject: Update on JFK SSI Information
Date: Fri Oct 31 2014 15:00:38 EDT
Attachments:

Sir,

I spoke to Sharon Huiswoud, my Information Systems Director, concerning the &#8220;Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport&#8221; (14-082-ITA-DHS). TSA&#8217;s Office of SSI representative, Robert Metzler, plans to provide us with a formal response/determination concerning all of the SSI comments that were provided to us in TSA&#8217;s technical comments. (I&#8217;m not sure why TSA&#8217;s SSI comments didn&#8217;t go through its SSI office before the comments were sent to us.) Once received, Nancy Eyl and our audit team will look over the points and come up with our own determinations/suggestions. We should be able to provide you with our determinations/suggestions by this coming Tuesday.

Rick

Richard Harsche

Acting AIG for IT Audits

Director, Information Management Division

Office of Inspector General

Department of Homeland Security

Phone: 202-254(b)(6)

E-Mail:(b)(6)@oig.dhs.gov <mailto(b)(6)@dhs.gov>

Cell: 202-

From: Roth, John </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) oig.dhs.gov747>
To: Morales, Arlen </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cr (b)(6) .dhs.gov>
Cc: Balaban, Dorothy </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>;
Hillburg, William </o=dhs/ou=exchange administrative group
(fydibohf23spdlt)/cn=recipients/cr (b)(6) oig.dhs.gov
085>
Bcc:
Subject: RE: JFK presser(2)
Date: Tue Dec 23 2014 09:56:30 EST
Attachments:

Good point. If it goes out before December 31, we are OK. In any event, we can say &#8220;Pistole did not respond.&#8221;

From: Morales, Arlen
Sent: Tuesday, December 23, 2014 9:09 AM
To: Roth, John
Cc: Balaban, Dorothy; Hillburg, William
Subject: FW: JFK presser(2)

Good Morning Mr. Roth,

Hope this email finds you well.

Should we edit the JFK presser since Mr. Pistole will retire?

Thank you.

IG Protests TSA&#8217;s Edits of Audit Report

Inspector General John Roth of the Department of Homeland Security (DHS) has protested actions by Transportation Security Administration (TSA) officials requiring the deletion of material in a new Office of Inspector General (OIG) report. During their review of the OIG&#8217;s Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport, TSA officials classified sections of the report as Sensitive Security Information (SSI). By law, m

Document ID: 0.7.368.5026

From: Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
To: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
Cc:
Bcc:
Subject: RE: memo to Doug Blair re JFK SSI
Date: Tue Nov 18 2014 11:19:57 EST
Attachments:

Dottie,

We would like Mr. Roth to send the memo to:

John S. Pistole

Administrator

Transportation Security Administration

Please copy:

Doug Blair

Sensitive Security Information Office Chief

Department of Homeland Security

Again, please let me know if the IG would like us to provide him with any additional assistance.

Rick

From: Balaban, Dorothy
Sent: Tuesday, November 18, 2014 11:09 AM
To: Harsche, Richard
Subject: RE: memo to Doug Blair re JFK SSI

I believe the IG was waiting for ITA to make a determination as to whom the memo should be addressed to.

Dottie

Dottie Balaban

Special Assistant to the Inspector General

Office of Inspector General

202-254 (b)(6)

Notary Public for the District of Columbia

From: Harsche, Richard
Sent: Tuesday, November 18, 2014 9:25 AM
To: Balaban, Dorothy
Subject: FW: memo to Doug Blair re JFK SSI

Dottie,

Do you know th

Document ID: 0.7.368.5014

From: Roth, John </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) oig.dhs.gov747>
To: Rimon, Laurel </o=dhs/ou=exchange
administrative group
(fydibohf23spdlt)/cn=recipients/cn= (b)(6) .oig.dhs.gova50>
; Balaban, Dorothy </o=dhs/ou=exchange administrative group
(fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
Cc:
Bcc:
Subject: RE: JFK CCTV
Date: Fri Apr 08 2016 07:32:21 EDT
Attachments:

Also, the first sentence should read: &#8220;Pursuant to Office of Management and Budget Circular A-50 (Revised), DHS Management Directive 077-01, and DHS Delegation Number 00109,

From: Rimon, Laurel
Sent: Friday, April 08, 2016 7:08 AM
To: Balaban, Dorothy
Cc: Roth, John
Subject: JFK CCTV

Dottie,

Attached is a memo from the IG to USM. It has my edits in track changes and needs to be put on letterhead and probably have these attachments incorporated. If you wouldn&#8217;t mind getting it in final form, we can both take a final look before it&#8217;s ready to go out.

Thanks,
Laurel

Document ID: 0.7.368.5005

From: Roth, John </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cr(b)(6)oig.dhs.gov747>
To: McCauley, Sondra </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)oig.dhs.govdab>
Cc: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>; Huiswoud, Sharon </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cr(b)(6)dhs.gov>; Paulson, Erica </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn(b)(6).dhs.gov>; Rimon, Laurel </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn(b)(6)oig.dhs.gova50>; Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cr(b)(6)dhs.gov>
Bcc:
Subject: RE: cover letter for JFK
Date: Fri Jan 16 2015 10:20:13 EST
Attachments:

Very helpful, thanksl.

From: McCauley, Sondra
Sent: Friday, January 16, 2015 9:38 AM
To: Roth, John
Cc: Balaban, Dorothy; Huiswoud, Sharon; Paulson, Erica; Rimon, Laurel; Harsche, Richard
Subject: RE: cover letter for JFK

Attached are my track change edits to the letter. I reviewed and approved the newly redacted version of the report with the team yesterday. I see that the redacted report was routed via PTS to Counsel and is now with CC_IG.

Let me know if you have questions about my attached edits.

Thanks,

Sondra McCauley

Assistant Inspector General for Information Technology Audits

Department of Homeland Security

Office of Inspector General

Work: 202-254 (b)(6)

Cell: 202-425 (b)(6)

(b)(6) @oig.dhs.gov

From: Roth, John
Sent: Thursday, January 15, 2015 5:58 PM
To: Paulson, Erica; Rimon, Laurel; Harsche, Richard; McCauley, Sondra
Subject: cover letter for JFK

I took a whack at editi

Document ID: 0.7.368.5017

From: Huiswoud, Sharon </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
To: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn= (b)(6) hs.gov>
Cc:
Bcc:
Subject: Meeting with the IG on JFK Report
Date: Thu Nov 06 2014 11:37:09 EST
Attachments:

Hi Dottie-

Rick would like to have the meeting on Monday. I am off that day but my team Sharell Grady and Beverly Dale will attend the meeting with him. What time on Monday is good for Mr. Roth?

Sharon L. Huiswoud

Director

Information Systems Division

Office of IT Audits

Department of Homeland Security

Office of Inspector General

office: 202-25 (b)(6)

cell: 202-49 (b)(6)

Document ID: 0.7.368.5012

From: Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
To: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
Cc:
Bcc:
Subject: FW: memo to Doug Blair re JFK SSI
Date: Tue Nov 18 2014 11:21:47 EST
Attachments:

Dottie,

I should have copied you on this email exchange with Mr. Roth on Friday.

Rick

From: Harsche, Richard
Sent: Friday, November 14, 2014 4:19 PM
To: Roth, John
Subject: Re: memo to Doug Blair re JFK SSI

As this is an issue concerning TSA's improper use of SSI, I would appreciate your weight on this one. We will address the memo to Mr. Pistole, from you.
Thanks,
Rick

From: Roth, John
Sent: Friday, November 14, 2014 04:01 PM
To: Harsche, Richard
Cc: Balaban, Dorothy
Subject: RE: memo to Doug Blair re JFK SSI

Yes, I meant SSI, but clearly my mind is still on my last meeting, in which we were talking about PII.

In reflecting on this, if we are going to stick with the current addressee, you should sign the memo. If it is addressed to Pistole, I will sign it. Just as a matter of protocol, and I am agnostic about which it should be.

From: Harsche, Richard
Sent: Friday, November 14, 2014 11:29 AM
To: Roth, John

Document ID: 0.7.368.5011

From: Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
To: Roth, John </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=(b)(6)oig.dhs.gov747>
Cc: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
Bcc:
Subject: FW: Technical Comments for “Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport” (14-082-ITA-DHS)
Date: Thu Oct 30 2014 17:03:48 EDT
Attachments:

Sir,

Just to keep you in the loop. Please see my responses to requests coming from the DHS GAO/OIG Liaison, Jim Crumpacker. TSA is really pushing hard on trying to get us to redact portions of the JFK report.

Rick

From: Harsche, Richard
Sent: Thursday, October 30, 2014 4:59 PM
To: Crumpacker, Jim
Cc: Huiswoud, Sharon; Schaeffer, Shelly; Schamberger, Steven; WHITE, ROBIN A; Mathias, Susan; Brothers, Christopher; Mayfield, Peggy; Seaman, Matthew
Subject: RE: Technical Comments for &#8220;Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport&#8221; (14-082-ITA-DHS)

Jim,

As part of our process, we ask that the Department inform us of areas for potential redaction. This includes markings such as LES and FOUO. There is a process in place that requires redaction requests to come from a senior DHS official with sufficient political accountability, and understanding of the purpose and role of our reports, and the ability to balance t

Document ID: 0.7.368.5007

From: Grady, Sharell </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
To: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
Cc: Huiswoud, Sharon </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>; Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn (b)(6) dhs.gov>
Bcc:
Subject: RE: Memo on Formal Request to Challenge SSI Office.docx
Date: Thu Nov 13 2014 15:09:45 EST
Attachments:

Password:

Tya8*tya

Sharell Grady
Audit Manager
DHS/OIG/Office of IT Audit
Information Systems Division
Office: 202 25 (b)(6)
Blackberry: 202 36 (b)(6)

Document ID: 0.7.368.5010

From: Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
To: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
Cc:
Bcc:
Subject: FW: memo to Doug Blair re JFK SSI
Date: Tue Nov 18 2014 09:24:31 EST
Attachments:

Dottie,

Do you know the status of this memo? Is there anything that the IG would like us to do?

Rick

From: Roth, John
Sent: Friday, November 14, 2014 4:02 PM
To: Harsche, Richard
Cc: Balaban, Dorothy
Subject: RE: memo to Doug Blair re JFK SSI

Yes, I meant SSI, but clearly my mind is still on my last meeting, in which we were talking about PII.

In reflecting on this, if we are going to stick with the current addressee, you should sign the memo. If it is addressed to Pistole, I will sign it. Just as a matter of protocol, and I am agnostic about which it should be.

From: Harsche, Richard
Sent: Friday, November 14, 2014 11:29 AM
To: Roth, John
Cc: Balaban, Dorothy
Subject: RE: memo to Doug Blair re JFK SSI

Sir,

I checked with the team and they advised that the memo does not contain SSI. Therefore, there is no need to mark it as such. We also believe that the memo is going to the appropriate person/level. We could/sh

Document ID: 0.7.368.5006

From: Roth, John </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)oig.dhs.gov747>
To: Harsche, Richard </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6).dhs.gov>
Cc: Balaban, Dorothy </o=dhs/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=(b)(6)dhs.gov>
Bcc:
Subject: memo to Doug Blair re JFK SSI
Date: Fri Nov 14 2014 10:58:42 EST
Attachments:

Nice memo. I signed it and didn&#8217;t have any edits.

After I signed it, some things came to mind, though: 1) is there any potential PII within the memo? If so, do we need to appropriately mark the memo?; 2) who should this be addressed to? Pistole is the ultimate decider &#8211; given that it is coming from me, and our compressed time frame, should we skip the intermediate steps? If not, he should at least be copied; 3) should we request a time period by which this decision should be made? It strikes me that this is a fairly narrow analysis that could be completed very quickly. 4) should we be explicit about our next steps (i.e., issue a redacted report with a note as to their PII determination, and our belief that this is being done for an improper purpose, but continue to seek review (this assumes we don&#8217;t get an answer from Pistole in a reasonable time))? To that end, we many consider the memo as an attachment, assuming it doesn&#8217;t contain any PII.